НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
___Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Методика проведення аудиту інформаційної безпеки у відповідності до ISO/IEC 27001:2015»

Виконав:
студент IV курсу, групи ТС-61
Андрійчук Андрій Анатолійович _____

Керівник:
Професор кафедри ТС, д.т.н., професор
Горицький Віктор Михайлович _____

Рецензент:
Старший викладач СК 5 ІСЗЗІ КПІ
Мітін Сергій Вячеславович _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент (-ка) _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Програма професійного спрямування (спеціалізація) – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

____ Леонід УРИВСЬКИЙ

«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Андрійчук Андрій Анатолійович

1. Тема роботи «Методика проведення аудиту інформаційної безпеки у відповідності до ISO/IEC 27001:2015», керівник роботи Горицький Віктор Михайлович, професор кафедри ТС, затверджені наказом по університету від 30 березня 2020 р. № 924-с

2. Термін подання студентом роботи 10 червня 2020

3. Зміст роботи

1) Системи управління інформаційною безпекою та їх місце в національній та глобальній інфраструктурі якості.

2) Системи менеджменту(управління) інформаційною безпекою на основі стандарту ISO/IEC 27001

3) Дослідження проблем впровадження та сертифікації СУІБ на основі ISO/IEC 27001

4) Висновки

4. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Презентація-захист на тему: «Методика проведення аудиту інформаційної безпеки у відповідності до ISO/IEC 27001:2015»

5. Дата видачі завдання 17. 11. 2019

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання	19.11.2019 – 25.11.2019	
2	Визначення мети дипломної роботи. Розробка змісту	27.11.2019 – 30.11.2019	
3	Написання вступної частини	10.12.2019 – 15.12.2019	
4	Написанні першого розділу	15.12.2019 – 05.01.2020	
5	Написання другого розділу	17.01.2020 – 30.01.2020	
6	Збір інформації для третього розділу	07.02.2020 – 03.03.2020	
7	Написання третього розділу	04.03.2020 – 25.03.2020	
8	Написання висновків, та загального висновку дипломної роботи	15.04.2020 – 19.04.2020	
9	Оформлення дипломного проекту	06.05.2020 – 16.05.2020	
10	Підготовка презентації для захисту	23.05.2020 – 30.05.2020	

Студент Андрій АНДРІЙЧУК
Керівник роботи Віктор ГОРИЦЬКИЙ

РЕФЕРАТ

Текстова частина дипломної роботи: 66 с., 9 рис., 4 табл., 17 джерел.

Метою роботи є дослідження систем управління інформаційною безпекою на основі міжнародного стандарту інформаційної безпеки ISO/IEC 27001.

В роботі розглядається міжнародний стандарт безпеки інформаційних технологій ISO/IEC 27001. Розглядається історія створення та його впровадження в інформаційні системи, структура цього стандарту а також все сімейство стандартів ISO/IEC 27x. Рівень на якому даний стандарт впроваджений на території України проблематика його впровадження та вдосконалення в національній системі інформаційної безпеки.

БЕЗПЕКА ІНФОРМАЦІЇ, ЗАХИСТ ІНФОРМАЦІЇ, ЗАПОБІГАННЯ РИЗИКІВ, ОРГАНИ ОЦІНКИ ВІДПОВІДНОСТІ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ABSTRACT

The aim of the work is to study information security management systems based on the international standard of information security ISO / IEC 27001.

The paper considers the international standard of information technology security ISO / IEC 27001. The history of its creation and implementation in information systems, the structure of this standard and the whole family of standards ISO / IEC 27x are considered. The level at which this standard is implemented in Ukraine is the issue of its implementation and improvement in the national information security system.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IAF	IAF - International Accreditation Forum
ILAC	International Laboratory Accreditation Cooperation
БДА	Бюро державної акредитації
СУІБ	Система управління інформаційною безпекою
ISMS	Information Security Management System
DTI	Department of Trade and Industry (Міністерство торгівлі і промисловості Великобританії)
BS	British Standard
BSI	British Standards Institution
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ARPANET	Мережа розширених дослідницьких проектів
CERT	Команда реагування на надзвичайні ситуації
NSA	Агенції національної безпеки
NBA	Network Behavioral Analysis
WAF	Брандмауери веб-додатків
DoS	Відмови у наданні послуг
OECD	Organisation for Economic Co-operation and Development.
OSN	Orbit Showtime Network
G7	Вели́ка сі́мка.
PDCA	(Plan-Do-Check-Act) планування, виконання, перевірка, вплив
ITIL	Information Technology Infrastructure Library
OGC	портфоліо кращих практик
CoBIT	Control Objectives for Information and related Technology
ISACA	Information Systems Audit and Control Association
ISM3	Information Security Management

FVEY	Five Eyes розвідувальний альянс, до якого входять такі країни: Австралія, Канада, Нова Зеландія, США та Велика Британія.

ВСТУП

Сучасний світ неможливо уявити без Інтернету. Доступ до інтернету зараз є у всі та скрізь, де б ти не був чи то вдома, чи на роботі, у транспорті та парках, ресторанах та кафе. Майже кожна людина, в сучасному світі, користується однією, двома а то й трьома різними соціальними мережами, месенджерами та акаунтами в різних службах доставки їжі, таксі та інших. Беручи до уваги вищесказане, постає проблема збереження особистих даних у безпеці.

В процесі розвитку інформаційних технологій, паралельно розвивається сфера інформаційної безпеки. За останні декілька десятиліть було вироблено десятки різних методів та практик захисту інформації, які зібрані до купи в системах управління інформаційною безпеки. Користуючись цими практиками, спеціалісти з інформаційної безпеки можуть ефективно реагувати та протидіяти сучасні загрозам, що виникають в інформаційній сфері.

Одним з таких методів є міжнародний стандарт інформаційної безпеки ISO/IEC 27001. Він увібрав у себе найкращі практики з організації управління інформаційною безпекою та найкращі методи протидії ризикам.

Впровадження даного стандарту в національну систему інформаційної безпеки допоможе державі в максимально швидких строках реагувати на різного роду загрози в інформаційному середовищі. Дотримання саме цього стандарту – великий крок до визнання перед світовим товариством а також покращує економічні показники країни.

Виходячи з цього, тема роботи є актуальною на сьогодні.

Метою роботи являється ознайомлення з стандартом ISO/IEC 27001 та сімейством стандартів ISO/IEC 27k . Визначення його ролі у світовій системі інформаційної безпеки та системі ІБ України.

Дослідження проблематики впровадження ISO/IEC 27001 в Україні.

Об’єктом дослідження є методики проведення аудиту інформаційної системи на основі стандарту ISO/IEC 27001.

1 СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ЇХ МІСЦЕ В НАЦІОНАЛЬНІЙ ТА ГЛОБАЛЬНІЙ ІНФРАСТРУКТУРІ ЯКОСТІ

1.1 Інфраструктура якості

Створення системи інфраструктури якості є одним з найкращих практичних кроків, які країна, що розвивається може зробити на своєму шляху для розвитку та процвітання економіки, добробуту і здоров'ю громадян. Система інфраструктури якості сприяє реалізації державної політики щодо розвитку різних сфер, включаючи промисловість, підвищення конкурентоспроможності на світових ринках, ефективне використання природних і людських ресурсів, безпеку продуктів харчування, здоров'я, навколишнє середовище та зміна клімату. Система інфраструктури якості пропонує повний пакет послуг, що враховує потреби всіх громадян країни - клієнтів і споживачів, а також підприємств і організацій, які пропонують продукти та послуги. Система інфраструктури якості включає в себе всі основні аспекти розвитку, в тому числі стратегії, інституційні основи, перелік постачальників послуг, при цьому спираючись на використанні міжнародних стандартів і процедур оцінки.

Система інфраструктури якості являє собою поєднання ініціатив, установ, організацій, діяльності та населення. Вона включає в себе національну політику в галузі розвитку якості і інститути її реалізації, роботу з нормативно-правовою базою, постачальників послуг, підприємства, клієнтів і споживачів (що має на увазі громадян як «споживачів» державних «послуг»).

Що ми розуміємо під визначенням «якості»? «Якість», в нашій уяві, - це робота над забезпеченням відповідності продуктів і послуг вимогам споживачів. Більш розгорнуто, під «якістю» розуміється те, що продукти і послуги повинні бути придатними для цілей, для яких вони заявлені. Наприклад, дорогі шкіряні черевики можна розглядати як предмет розкоші, але вони не будуть відповідати вимогам якості, виставленим фермером. Для

останнього більш краща пара набагато менш дорогих гумових чобіт, придатних для роботи в сільських умовах. Саме цим сприйняттям поняття «якості», як відповідність цілям і задоволення вимог замовника, і буде оперувати системою інфраструктури якості з метою ефективного досягнення результатів у вирішенні широкого кола завдань - і не тільки по відношенню до товарів або послуг. Прикладами можуть поняття, які представляють інтерес для розвиваючих країн - безпека харчових продуктів, якість охорони здоров'я, якість захисту навколишнього середовища, боротьба зі зміною клімату, якість соціальної захищеності і якість вирішення питань, пов'язаних з гендерною нерівністю.

Система інфраструктури якості (СІЯ) - це динамічна система з фокусом на дію. Дія, в свою чергу, спрямована на досягнення результатів і їх оцінку. «Система» означає, що всі складові частини взаємопов'язані для забезпечення загального результату роботи СІЯ, який являє собою багатьом більше, ніж можна досягти при використанні підрозділів, що працюють в індивідуальному порядку.

Система інфраструктури якості є каталізатором поліпшення якості продукції і послуг в національному масштабі. Саме тому вона допомагає стимулювати загальний попит на товари і послуги, що буде «підганяти» окремі підприємства, а отже, і економіку в цілому. Допомагаючи національної промисловості задовольняти вимоги експортних ринків, СІЯ максимально підвищує конкурентоспроможність економіки країни і її здатність брати участь у світовій торгівлі.

Система інфраструктури якості є потужним інструментом для визначення, розробки та перевірки вимог до якості товарів і послуг. Вона досліджує і доводить факти відповідності вимогам якості, виставленим щодо продуктів і послуг. Система інфраструктури якості гарантує відповідність вимог до якості послуг, продуктів і послуг вимогам, які впроваджені та практикуються в міжнародній торгівлі.

Не буває стандартної моделі системи інфраструктури якості, яка підходила б для всіх країн одночасно, необхідний персональний підхід по кожній з практик. Система інфраструктури якості регулюється відповідно до національних та регіональних вимог, які повинні бути виявлені шляхом ретельної оцінки існуючих потреб. Використання інфраструктури якості створює переваги по всьому ланцюжку попиту-пропозиції, включаючи такі складові, як Споживач, Виробник і Постачальник.

– Споживач отримує свою вигоду, виходячи з того, що інфраструктура якості забезпечує впевненість в тому, що продукти і послуги відповідають його вимогам.

– Виробник і Постачальник також отримують свою вигоду, оскільки система сприяє використанню міжнародних стандартів для забезпечення відповідності їх продуктів і послуг встановленим вимогам, так само як і відповідності їх бізнес-процесів - міжнародним системам менеджменту.

– Вигода Регуляторів в тому, що інфраструктура якості допомагає визначати стандарти і процеси оцінки відповідності, щоб гарантувати задоволення всім вимогам щодо захисту інтересів суспільства, таких як охорона здоров'я, безпека та захист навколишнього середовища. Регулятор може зробить оцінку відповідності обов'язковим в цих областях і може заборонити продаж продуктів і послуг які не відповідають вимогам.

– Уряд також отримує користь, так як інфраструктура якості включає в себе систему стимулювання економіки і підвищення конкурентоспроможності промисловості на світових ринках, а також досвід ефективного використання ресурсів, обміну технологічними ноу-хау, вирішення екологічних і кліматичних проблем, а також приклади ефективного управління в сферах суспільної охорони здоров'я і безпеки, включаючи безпеку харчових продуктів.

Послуги інфраструктури якості

Однією з ланок у ланцюзі системи інфраструктури якості є організації, що надають послуги з оцінки відповідності для всієї інфраструктури якості.

Оцінкою відповідності називається сукупність процесів і процедур, які використовуються для демонстрації того, що продукт або послуга, їх управління, організація або персонал відповідає встановленим вимогам. Ці вимоги, як правило, викладені в міжнародних стандартах, розроблених такими організаціями, як ISO (Міжнародна організація по стандартизації). Вимоги, що пред'являються до діяльності по оцінки відповідності, самі по собі також наведені в міжнародних стандартах, і це допомагає забезпечити узгодженість у всьому світі, а також міжнародне прийняття результатів. Використання міжнародних стандартів, гармонізує діяльність з оцінці відповідності з усього світу. Це дає величезні вигоди для міжнародної торгівлі в цілому. Угоди між країнами або регіонами по взаємному визнанню вимог, методів оцінки, інспекції або результатів випробувань та інше - все це може допомогти скоротити або усунути технічні бар'єри в торгівлі. Це - вимоги і правила з регулювання імпорту та доступу до ринків. Ситуація з ринками варіюється від країни до країні, і без необхідної глобальної домовленості завжди буде можливість усунути іноземний продукт від входу в національний ринок. На рис.1.1 схематично зображено всю лінію інфраструктури якості.

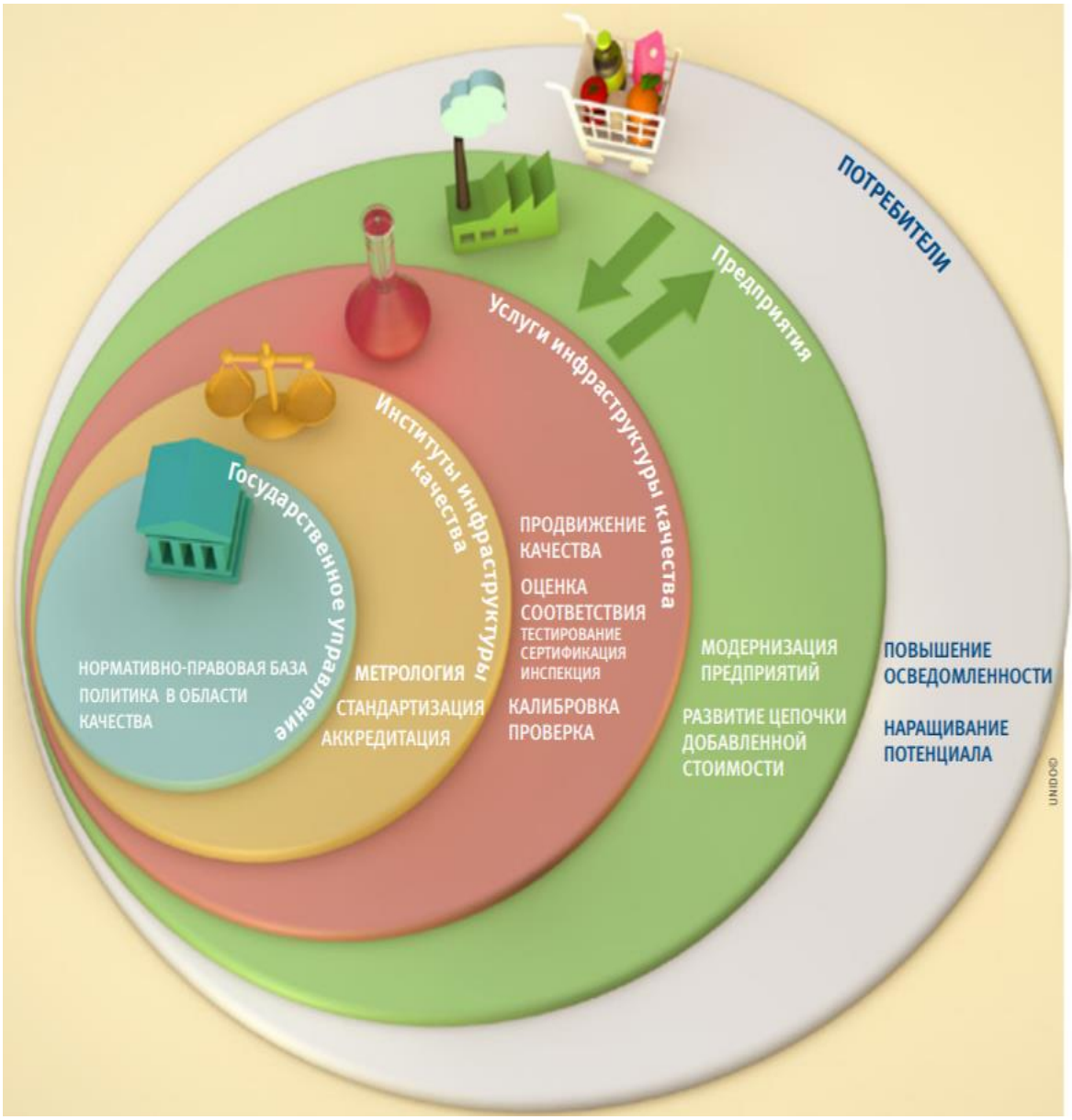

Рисунок1.1 - Інфраструктура якості[18]

Інспекція.

Перевіряючі органи відіграють істотну роль в транскордонній торгівлі. Вони діють від імені урядів і ділових партнерів (імпортерів і експортерів) шляхом перевірки імпортованих товарів і матеріалів. Вони несуть відповідальність за розгляд величезного асортименту продукції, матеріалів, виробництва, установок, процесів, процедур, робіт і послуг, як в приватному, так і в державному секторі. Вони повинні інформувати про такі параметри, як якість, придатність для використання і постійна безпеку при експлуатації.

Мета їх роботи полягає в тому, щоб зменшити ризик для всіх - покупця, власника, користувача або споживача вироби, що підлягає перевірці. Уряд і бізнес часто використовують послуги для перевірки імпортованих товарів і матеріалів.

Сертифікація.

Сертифікацією називається підсумок процесів, що завершується видачею органом по сертифікації письмової гарантії того, що продукт, послуга, процес, персонал, організація або система управління відповідає конкретним вимогам.

Стандартизація.

У кожного з нас є певні очікування від продуктів і послуг, які ми купуємо і використовуємо. Ми очікуємо, що вони повинні бути застосовні для зазначених цілей, безпечні і прості у використанні, не нести шкоди здоров'ю або навколишньому середовищу; вони повинні бути надійними і ефективними, взаємозамінні і сумісні з іншими продуктами і, нарешті, повинні залучати ціною. Стандарти - це задокументовані угоди, які переводять бажані характеристики в вимірювання, вага, процеси, системи, передові практики та інші якості, з тим, щоб продукти та послуги відповідали вимогам, забезпечуючи впевненість покупців і користувачів. Для країн, що розвиваються міжнародні стандарти, розроблені на основі всесвітнього консенсусу експертів в цій області, є важливим джерелом технологічних ноу-хау. Визначивши характеристики, якими повинні володіти продукти і послуги для відповідності вимогам експортних ринків, міжнародні стандарти надають країнам, що розвиваються основу для прийняття правильних рішень при інвестуванні своїх ресурсів. У структурі системи інфраструктури якості, стандартизацією, як правило, займаються Національні бюро стандартизації (НБС), які можуть представляти інтереси країн в таких організаціях, як ISO (Міжнародна організація по стандартизації). НБС можуть надати національним делегаціям право брати участь в розробці стандартів, що мають ключове значення для економіки країни. Незалежно від участі НБС в

розробці стандарту, національне бюро може вільно переводити на національну мову і приймати міжнародні стандарти як національні стандарти. Використання міжнародних стандартів гарантує витяг країною вигод з передового світового досвіду, а також відповідність місцевої продукції вимогам експортерів. Для споживачів відповідність продукції і послуг міжнародним стандартам є гарантією їх якості, безпеки і надійності.

Метрологія.

Метрологія, або наука про вимірювання, є життєво важливою частиною нашого повсякденного життя. Наприклад, їжа купується за вагою, вода і електрика дозуються, інструменти для аналізу зразків крові повинні бути точними. Очевидно, що помилки при вимірюванні з використанням медичних приладів або в обслуговуванні критичних компонентів, таких як автомобільні гальма або авіаційні двигуни, можуть бути життєво важливими. Точні виміри і вимірювальні прилади необхідні для захисту здоров'я та безпеки споживачів і охорони навколишнього середовища. Елементи метрології також грають важливу роль в договорах, як між діловими партнерами, так і в світовій торгівлі в цілому. Ваги і інші інструменти в лабораторіях повинні бути відкалібровані для забезпечення надійності і точності вимірювань. Підприємства не можуть реалізувати процес управління виробництва згідно зі стандартними характеристиками, якщо контрольні прилади, такі, наприклад, як прилади вимірювання тиску і температури, що не відкалібровані. Надійність національної системи заходів забезпечується національними інститутами метрології (НИМ) щодо підписання акту про взаємне визнання Міжнародного комітету мір і ваг (CIPM MRA). Ця домовленість представляє організаційну і технічну базу для надання сприяння НИМ у визнанні еталонів і сертифікатів калібрування - невід'ємними елементами світової торгівлі.

Акредитація.

Акредитацією є процес, за допомогою якого авторитетний орган дає формальне визнання компетентності організації або приватної особи у

виконанні конкретних завдань. У структурі систем якості, відділ відповідальний за акредитацію оцінює компетенцію органів сертифікації продукції, системи менеджменту і персоналу, випробувальних і контрольних лабораторій. Офіційне визнання, іменоване «акредитацією», засвідчує клієнтам і користувачам послуг компетентність діяльності даних організацій. Акредитація часто входить в мандат Бюро державної акредитації (БДА), які можуть забезпечити визнання своїх послуг з акредитації в рамках Міжнародного форуму з акредитації (IAF) і Міжнародної лабораторії форуму з акредитації (ILAC). IAF і ILAC сприяють і управляють визнанням «двосторонніх» або «багатосторонніх» «угод» або «домовленостей» (MPA), згідно з якими беруть участь сторони погоджуються обопільно визнавати результати тестування, інспекцій, сертифікації або акредитації. MPA може стати важливим кроком на шляху оптимізації числа оцінок продуктів, послуг, систем, процесів і матеріалів, необхідних особливо в міжнародній торгівлі.

1.2 Системи менеджменту/управління інформаційною безпекою. Історичний огляд розвитку

Сьогодні безпеку цифрового простору показує новий шлях національної безпеки кожної країни. Відповідно до ролі інформації як цінного товару в бізнесі, її захист, безумовно, необхідний. Для досягнення цієї мети, кожної організації, в залежності від рівня інформації (з точки зору економічної цінності), потрібна розробка системи управління інформаційною безпекою (далі - СУІБ), поки існує можливість, захисту своїх інформаційних активів.

В організаціях, існування яких в значній мірі залежить від інформаційних технологій, можуть бути використані всі інструменти для захисту даних. Проте, безпека інформації необхідна для споживачів, партнерів по співпраці, інших організацій а також для уряду. У зв'язку з цим,

для захисту цінної інформації, необхідно що б кожна організація прагнула до тієї чи іншої стратегії та реалізації системи безпеки на її основі.

СУІБ є частиною комплексної системи управління, заснованої на оцінці та аналізів ризиків, для розробки, реалізації, адміністрування, моніторингу, аналізу, підтримки та підвищення інформаційної безпеки і її реалізації, отриманих з цілей організації і вимоги, вимоги безпеки, які використовуються процедур і розмірах і структурі її організації.

Зародження принципів і правил управління ІБ почалося в Великобританії в 1980-х роках. Тоді Міністерство торгівлі і промисловості Великобританії (англ. Department of Trade and Industry, DTI) організувало робочу групу для розробки збірки кращих практик щодо забезпечення ІБ.

У 1989 році «DTI» опублікувало перший стандарт в цій області, який називався PD 0003 «Практичні правила управління ІБ». Він представляв собою перелік засобів управління безпекою, які в той час вважалися адекватними, нормальними і хорошими, застосовними до технологій того часу. Документ «DTI» був опублікований як керівний документ британської системи стандартів (англ. British Standard, BS).

У 1995 році Британський інститут стандартів (англ. British Standards Institution, BSI) прийняв національний стандарт BS 7799-1 «Практичні правила управління ІБ». Він описував 10 областей і 127 механізмів контролю, необхідних для побудови СУІБ (англ. Information Security Management System, ISMS), визначених на основі кращих світових практик.

Цей стандарт і став прабатьком всіх міжнародних стандартів СУІБ. Як і будь-який національний стандарт BS 7799 в період 1995-2000 років користувався помірною популярністю тільки в рамках країн британської співдружності.

У 1998 році з'явилася друга частина цього стандарту - BS 7799-2 «СУІБ. Вимоги та настанови щодо застосування », що визначив загальну модель побудови СУІБ і набір обов'язкових вимог, на відповідність яким повинна проводитися сертифікація. З появою другої частини BS 7799, що

визначила, що повинна з себе представляти СУІБ, почався активний розвиток системи сертифікації в галузі управління безпекою.

В кінці 1999 року експерти Міжнародної організації зі стандартизації (англ. International Organization for Standardization, ISO) і Міжнародної електротехнічної комісії (англ. International Electrotechnical Commission, IEC) прийшли до висновку, що в рамках існуючих стандартів відсутній спеціалізований стандарт управління ІБ. Відповідно, було прийнято рішення не займатися розробкою нового стандарту, а по погодженням з «BSI», взявши за базу BS 7799-1, прийняти відповідний міжнародний стандарт ISO / IEC.

В кінці 1999 року обидві частини BS 7799 були переглянуті і гармонізовані з міжнародними стандартами систем управління якістю ISO / IEC 9001 та екологією ISO / IEC 14001, а рік по тому без змін BS 7799-1 був прийнятий як міжнародний стандарт ISO / IEC 17799 2000 «Інформаційні технології (далі - IT). Практичні правила управління ІБ ».

У 2002 році була оновлена і перша частина стандарту BS 7799-1 (ISO / IEC 17799), і друга частина BS 7799-2.

Що ж стосується офіційної сертифікації по ISO / IEC 17799, то вона спочатку не була передбачена (повна аналогія з BS 7799). Була передбачена тільки сертифікація по BS 7799-2, який представляв собою ряд обов'язкових вимог (що не увійшли в BS 7799-1) і в додатку перелік умовно обов'язкових (на розсуд сертификатора) найбільш важливих вимог BS 7799-1 (ISO / IEC 17799).

Україна, а саме Національний Банк почав на практиці застосовувати вимоги міжнародного стандарту з 2008 року, поставивши за обов’язок всім місцевим банкам виконувати його вимоги, створюючи ситему управління ІБ на основі стандартів безпеки ISO.

У складі ISO / IEC за розробку сімейства міжнародних стандартів з управління ІБ відповідає підкомітет №27, тому була прийнята схема нумерації даного сімейства стандартів з використанням серії послідовних номерів, починаючи з 27000 (27k).

У 2005 році підкомітет SC 27 «Методи захисту IT» об'єднаного технічного комітету JTC 1 «IT» ISO / IEC розробив сертифікаційний стандарт ISO / IEC 27001 «IT. Методи захисту. СУІБ. Вимоги », що прийшов на зміну BS 7799-2, і тепер сертифікація проводиться вже по ISO 27001.

У 2005 році на основі ISO / IEC 17799 2000 був розроблений ISO / IEC 27002: 2005 «IT. Методи захисту. Звід норм і правил управління ІБ ».

На початку 2006 року був прийнятий новий британський національний стандарт BS 7799-3 «СУІБ. Керівництво з управління ризиками ІБ », який в 2008 році отримав статус міжнародного стандарту ISO / IEC 27005« IT. Методи захисту. Управління ризиками ІБ ».

У 2004 році Британським інститутом стандартів було опубліковано стандарт ISO / IEC TR 18044 «IT. Методи захисту. Управління інцидентами ІБ ». У 2011 році на його базі був розроблений стандарт ISO / IEC 27035 «IT. Методи захисту. Управління інцидентами ІБ ».

У 2009 році був прийнятий стандарт ISO / IEC 27000 «IT. СУІБ. Загальний огляд і термінологія ». Він надає огляд систем управління ІБ і визначає відповідні терміни. Словник ретельно сформульованих формальних визначень охоплює більшість спеціалізованих термінів, пов'язаних з ІБ і використовуваних в стандартах групи ISO / IEC 27.

25 вересня 2013 року було опубліковано нові версії стандартів ISO / IEC 27001 та 27002. З цього моменту стандарти серії ISO / IEC 27k (управління ІБ) повністю інтегровані до стандартів серії ISO / IEC 20k (управління IT-сервісами). Вся термінологія з ISO / IEC 27001 перенесена в ISO / IEC 27000, який визначає загальний термінологічний апарат для всього сімейства стандартів ISO / IEC 27k.

Інформаційна безпека пройшла дуже довгий шлях за останні півстоліття.

Починаючи з жарту між колегами ще в 1960-х, постійний підйом технологій у наступні роки зробив інформаційну безпеку величезною проблемою а від того і потребою сучасності.

Великі компанії, такі як Yahoo, Microsoft та Equifax, були атаковані хакерами мільйони разів лише протягом останніх десяти років. Крім того, хоча організація кібербезпеки за останні роки покращилася в рази, атака WannaCry "викупщиком" 2017 року підтвердила, що не лише інформаційна безпека розвивалася роками - хакери та комп'ютерні віруси теж є.

Проблема, безумовно, вже не є жартом, і, хоча компанії можуть фізично захищати свої файли за допомогою ряду технік безпеки та пожежної безпеки, наявність ефективного антивірусного програмного забезпечення є обов'язковим для запобігання кібератакам.

Ось детальний того, як інформаційна безпека, і хакерство еволюціїнували за весь час та етапи, які визначили їх прогресування:

- 1960-ті роки: Захист паролем

В 60-х, організації вперше стали більш захищати свої комп’ютери. В ті часи ще не було інтернету чи мережі для занепокоєння, тому безпека значною мірою була зосереджена на більш фізичних заходах та недопущенні доступу до людей, які мають достатньо знань щодо комунікувати з комп’ютером. Для цього було додано паролі та декілька шарів захисту безпеки до пристроїв. Також були вжиті заходи пожежної безпеки для забезпечення збереження збережених даних. Зрештою, в ті часи не було доступно iCloud, тому комп’ютери повинні були бути захищені іншими способами.

- 1970-ті роки: From CREEPER to Reaper

Історія кібербезпеки розпочалася з дослідницького проекту в 70-х роках, який тоді був відомий як ARPANET (Мережа розширених дослідницьких проектів). Дослідник на ім'я Боб Томас створив комп'ютерну програму, яка змогла перемістити мережу ARPANET, залишивши невеликий слід, куди б вона не пішла. Він назвав програму "CREEPER" через друковане повідомлення, яке було залишене під час подорожі по мережі: "Я КРІПЕР: ЗЛОВИ МЕНЕ, ЯКЩО МОЖЕШ".

Рей Томлінсон - людина, що винайшла електронну пошту - пізніше розробив програму, яка підняла CREEPER на наступний рівень, зробивши його самовідтворюваним та першим в історії комп'ютерним хробаком. На щастя, він написав ще одну програму під назвою Reaper, яка переслідувала CREEPER та видалила її, подавши перший приклад антивірусного програмного забезпечення.

Програми Томаса і Томлінсона, можливо, були розроблені як жарт, але вони насправді послужили надзвичайно важливою метою, виявивши ряд недоліків у мережевій безпеці ARPANET. У той час це викликало велике занепокоєння, оскільки багато великих організацій та урядів пов'язували свої комп'ютери по телефонних лініях, щоб створити власні мережі. Деякі групи людей почали також визнавати це, шукаючи шляхи проникнення в ці лінії та вкрадати важливі дані.

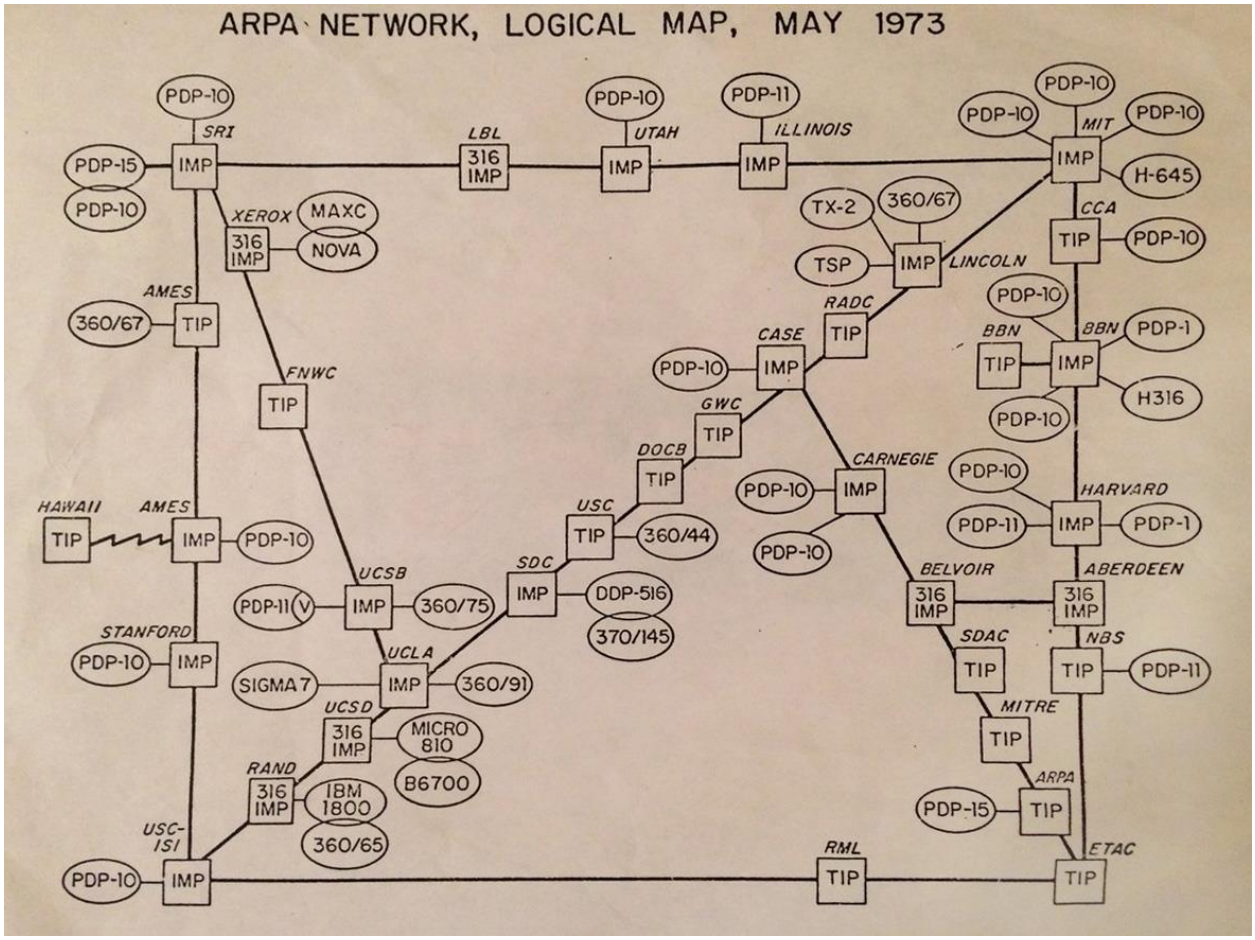

Рисунок 1.2 - Структура ARPANET [18]

– 1980-ті: Інтернет ошелешив

Далі комп’ютери почали ставати все більш підключеними до мереж, комп'ютерні віруси ставали все більш досконалими, а системи захисту інформації не могли йти в ногу з постійною забороною інноваційних підходів.

Наприклад, росіяни почали використовувати кіберпотужність як зброю і в 1986 році застосували німецького комп’ютерного хакера Маркуса Гесса для крадіжки військової таємниці США. Він зламав понад 400 військових комп'ютерів, включаючи мейнфрейми в Пентагоні, і вже хотів передати свої секрети КДБ, але його впіймали.

Через два роки, у 1988 році, відбувся народження Черв'яка Морріса - один з головних моментів в історії інформаційної безпеки. Використання мережі почало швидко збільшуватись, все більше університетів, військових органів та урядів стали підключатися до неї. Це означало, що заходи безпеки повинні також поступово ставати більш використовуваними.

Названий на честь свого винахідника Роберта Морріса, черв'як був розроблений для розповсюдження по мережах, проникнення в термінали, використовуючи помилку в мережі, а потім копіював себе. Її метою було виявити незахищені зони в системі захисту від вторгнення в мережу.

Шкода, яку вона завдавав черв’як, була настільки серйозною, що Роберт Морріс став першою особою, яка отримала звинувачення відповідно до Закону про комп'ютерні шахрайства та зловживання. У результаті була створена також Комп'ютерна команда реагування на надзвичайні ситуації (CERT), щоб запобігти виникненню кібер-проблем, подібних до таких.

– 1990-ті: підйом брандмауерів

Коли Інтернет стає доступним для громадськості, все більше людей починають розміщувати свою особисту інформацію в Інтернеті. Через це

суб'єкти організованої злочинності розглядали це як потенційне джерело доходу і почали красти дані у людей та урядів через Інтернет.

До середини 90-х загрози безпеки мережі зростали експоненціально, і, таким чином, брандмауери та антивірусні програми мали створюватися масово для захисту населення. Саме дослідник NASA створив першу програму брандмауера після атаки комп’ютерних вірусів на їх базу в Каліфорнії.

– 2000-ті: належне покарання

На початку 2000-х уряди почали стримувати інтернет злочинність, виносячи набагато більш серйозні звинувачення винним - включаючи великий термін ув'язнення та великі штрафи.

Інформаційна безпека продовжувала прогресувати, оскільки Інтернет розповсюджувався, на жаль разом і з віруси. Хакерам швидко вдалося створити віруси, які могли націлити не лише на конкретні організації, а й на цілі міста, штати і навіть континенти.

– 2010-ті: епоха великих порушень

Завдяки послідовному зростанню технологій, хакінг ставав все складнішим протягом наступних років, і низка основних витоків даних зараз значною мірою визначила епоху.

– Snowden & NSA, 2013. Едвард Сноуден - колишній працівник ЦРУ та підрядник уряду США - скопіював та просочив секретну інформацію з Агенції національної безпеки (NSA), підкресливши той факт, що уряд фактично "шпигує" для громадськістю. Він вважається героєм для одних і зрадником для інших.
– Yahoo, 2013 - 2014. Хакери зламали Yahoo, викравши облікові записи та особисту інформацію всіх своїх трьох мільярдів користувачів. Їх оштрафували на 35 мільйонів доларів за те, що не повідомили про порушення вчасно, а продажна ціна Yahoo знизилася на 350 мільйонів доларів.

– WannaCry, 2017. Більш широко відомий як перший "викуп", WannaCry орієнтувався на комп'ютери з операційною системою Microsoft Windows і вимагав виплат за викуп у криптовалюті Bitcoin. Лише за один день глист заразив понад 230 000 комп'ютерів у 150 країнах.

Хоча кожне з цих порушень даних було надзвичайно серйозним, на щастя, існує ряд компаній, які пропонують рішення для цих потенційних загроз - тому це не все погано.

Інформаційна безпека постійно вдосконалюється, і багато компаній розробляють широкий спектр варіантів зменшення атак для початківців, які використовують такі речі, як Network Behavioral Analysis (NBA), брандмауери веб-додатків (WAF) та захист відмови у наданні послуг (DoS).

Людям і підприємствам важливо підтримувати свою інформаційну безпеку та застосовувати методи для забезпечення їх захисту. Наприклад, якщо ви є бізнесом, використання експертного сервісу пошуку, зберігання та управління документами може забезпечити вам спокій, який ви прегнете знаючи, що ваші документи в безпеці. Так само використання хмарної платформи для зберігання ваших особистих файлів може бути рятівним, якщо ви коли-небудь втратите або пошкодите фізичні файли.

1.3 Стандартизація систем управління/менеджменту інформаційної безпеки

Історія інформаційної безпеки ІС йде далеко в минуле, починаючи близько 4000 років тому до нашої ери в Стародавньому Єгипті. Правителі, солдати, дипломати та підприємці в наступні тисячоліття зрозуміли важливість захисту інформації та починаючи з Другої світової війни ІС починає значний розвиток. Розвиток ІС та ІКТ вимагав додаткових заходів безпеки інформації: основні вимоги (забезпечення конфіденційності, цілісності, доступність) поступово посилювались новими. Поява нових ІС /

ІКТ спричинило появу нових загроз безпеці. ІС починає відігравати важливішу роль, тому створюються органи стандартизації для забезпечення належного рівня безпеки, приймаються найкращі практики безпеки. Таким чином, стандарти стали важливим інструментом досягнення необхідного рівня безпеки ІС. Це знайшло своє відображення в діяльність органів стандартизації, що випускають велику кількість нових стандартів, методологій, практик тощо, та поступово охоплює всю діяльність у сферах ІС / ІКТ управління в компаніях. Нині їх є велика кількість: стандарти серії ISO / IEC270xx, BS 7799, ITIL, PRINCE2, CoBIT, OPM3, CMMI, P – CMM, PCI DSS тощо. Таким чином, ІС стає важливою складовою безпеки компанії та вирішальним фактор покращення продуктивність компанії. Фактичне порушення ІС призводить до втрата довіри як ділових партнерів, так і клієнтів.

Управління безпекою ІС / ІКТ суттєво впливає на розвиток компанії. ІС є необхідною умовою ефективного результату діяльність компанії. У широкому розумінні це означає безпеку ІС та захист інформаційного простору і практично захист компанії. Міжнародний стандарт ISO / IEC 27001: 2015, надає інформацію про широкий спектр ризиків, щоб забезпечити безперервність бізнес процесів, мінімізувати втрати та максимізувати віддачу інвестиції. Європейський Союз та національні організації (OECD, OSN, G7 тощо) сприймають ІС як всесвітню проблему. Відповідно до стандарту BS 7799, СУІБ входить до складу загальної система управління, заснована на підході до ризиків, роль яких полягає у впровадженні, реалізації, експлуатації, контролювати, переглядати, підтримувати та вдосконалювати ІС.

Інформація - це зміст даних, що зустрічаються в різних формах: письмова, усна, графічна та електронна (цифрова) форми. Оскільки інформація є ключовим активом, загроза її безпеці створює серйозну проблему яку слід вирішувати швидко та ефективно. На практиці часто зустрічається комбіновані вимоги до захисту інформації.

Відповідно до ISO / IEC 27001: 2013 та ISO / IEC 27002: 2013, основні вимоги безпеки до даних є конфіденційність, цілісність, доступність, справжність, підзвітність та конфіденційність.

- Конфіденційність означає, що інформація надається та є доступною лише уповноваженим особам.
- Цілісність означає забезпечення правильності та повноти інформація за змістом та формою. Наявність інформація означає, що інформація доступна уповноваженим особам, коли їм це потрібно.
- Автентичність інформації полягає у забезпеченні цілісності та оригінальність документа. Простежуваність дозволяє визначити, який суб'єкт господарювання проводив питання щодо безпеки діяльності, наприклад хто ввів, змінив, видалив або прочитав інформацію.

Міжнародний стандарт ISO / IEC 27001, опублікований в 2002 році був переробленою версією BS 7799–2: 1999. У ньому описані основні вимоги до проектування, впровадження, експлуатації, моніторингу, огляду та вдосконалення СУІБ всередині компанії. Тут описано, як здійснювати контроль безпеки, адаптований до потреб організації або їх частини. Він також використовується для оцінки відповідності внутрішніх чи зовнішніх зацікавлених сторін та сертифікаційні перевірки. Є окремі специфікація для ISMS, повністю сумісні з уже створеними системи управління якістю відповідно до ISO 9001: 2008 або управління навколишнім середовищем відповідно до ISO 14001: 2004. Стандарт ISO / IEC 27001: 2013 може бути застосований у стандартах компаніях всіх типів і розмірів, а також в різних сферах бізнесу. Він розроблений таким чином, що дозволяє компаніям організовувати або інтегрувати свою ISMS відповідно до вимоги іншої системи управління. Стандарт ISO / IEC 27001: 2013 структурований у вісім глав та три додатки. Основна частина стандарту визначає обов'язкові частини СУІБ, особливо область оцінки ризику. Додаток до стандарт описує одинадцять областей управління на основі кращих практики в області:

1. Політика безпеки.

2. Організація інформаційної безпеки.

3. Управління активами.

4. Безпека людських ресурсів.

5. Фізична безпека та екологічна безпека.

6. Управління зв’язком та експлуатацією.

7. Управління підходами.

8. Придбання, розробка та обслуговування інформаційних систем.

9. Управління безпекою інцидентів.

10. Управління безперервним управлінням організації.

11. Дотримання вимог.

Міжнародний стандарт BS 7799 був виданий в 1995 році BSI. Він був розроблений для допомоги впровадженні ISMS в компанії, але не звертав великої уваги на виконання оцінок ризику. Розробка стандарту стала досягненням первинного рівня систем захисту інформації та стандартів безпеки управління. В 1998–1999 рр. стандарт було переглянуто та розширено до двох частини. BS 7799–1: 1998 - Кодекс практики інформації Управління безпекою. Стандарт був включений в систему міжнародних стандартів ISO без будь-яких істотні зміни, це заклало основу для розробки ISO / IEC 17799 (опубліковано у 2000 р.).

- BS 7799–2: 1999 - Специфікація інформаційної системи управління безпеки. Після його перегляду був виданий у 2002 році під назвою BS7799–2: 2002. Метою поправки було, узгодження його зі стандартом ISO 9001: 2008 система управління якістю та ISO 14001 система управління навколишнім середовищем та впровадження циклу PDCA. У 2005 році стандарт BS 7799–2: 2002 ліг в основу ISO / IEC 27001, опублікованого у 2005 році. BS 7799–3 був виданий у 2005 році (версія ISO від ISO / IEC 27005 - Управління інформаційною безпекою системи - рекомендації щодо ризику інформаційної безпеки управління). Стандарт узгоджується з іншими документи ISO / IEC, особливо з вищезгаданими стандарти ISO / IEC 17799: 2005 та ISO / IEC

27001: 2005. Він в основному надає рекомендації щодо виконання вимог, викладених в ISO / IEC 27001: 2005 щодо управління ризиками та пов'язаного з цим діяльності. Він достатньо загальний для використання у всіх компаніях незалежно від їх розміру.

ITIL (Information Technology Infrastructure Library) - це складна система томів, що залишають певну свободу в реалізації процесів. Належить до портфоліо кращих практик OGC. Це процес - орієнтований в основному на сферу управління IT послугами. Він підходить як для IT-сервісів постачальники, а також для великих підрозділів IT компатій. Він заснований на циклах PDCA. ITIL був розроблений і поступово публікується з 1980 року, як відповідь на вимогу британський уряд з метою забезпечення якості послуги та зменшення витрат на IT. У 1990 році ITIL був прийнятий великими компанії та урядовими установи Європи. Почалось поступово впроваджується до неурядових установ та організації у Великобританії та в усьому світі. В 2000 року Microsoft почала використовувати ITIL V1 як основу для розробки власних продуктів під назвою Microsoft Operations Framework. У 2001 році ITIL V1 було переглянуто. ITIL V2 складався з 10 частин: дві основні (Служба підтримки та надання послуг), які були поділені на кілька коротких томів та інші дев’ять. У 2006 році був опублікований словник ITIL. У 2007 році була опублікована розширена версія ITIL V3 (5 томів).

CoBIT (Control Objectives for Information and related Technology) - це фреймворк, розроблена в 1996 році міжнародною організаціжю ISACA для управління IT. Він включає в себе сукупність практик, що дозволяють досягти стратегічних цілей компаніям шляхом ефективного використання наявних джерела та мінімізація IT-ризиків. CoBIT - насамперед призначений для менеджерів, аудиторів та користувачів IT, що використовують її із системою процесів, показників та метрик які можна використовувати для впровадження системи IT управління з метою максимальної вигоди від IT

утилізація. CoBIT використовується для налаштування або аудиту інформаційні процеси у великих компаніях.

1.4 Висновки до розділу 1

В даному розділі було розглянуто наступні питання:

- Інфраструктура якості
- СУІБ, історичний огляд
- СУІБ як ключовий чинник успішної організації
- Стандартизація систем управління інформаційної безпеки

Система інфраструктури якості (СІЯ) - це динамічна система з фокусом на дію. Дія, в свою чергу, спрямована на досягнення результатів і їх оцінку. «Система» означає, що всі складові частини взаємопов'язані для забезпечення загального результату роботи СІЯ, який являє собою багатьом більше, ніж можна досягти при використанні підрозділів, що працюють в індивідуальному порядку. Система інфраструктури якості є каталізатором поліпшення якості продукції і послуг в національному масштабі. Саме тому вона допомагає стимулювати загальний попит на товари і послуги, що буде «підганяти» окремі підприємства, а отже, і економіку в цілому.

Історія створення СУІБ простягається далеко в часи ще єгипецьких імператорів. Вже тоді люди почали задумуватись про важливість безпеки інформації та методики забезпечення цієї безпеки. На сьогоднішній день, не можливо уявити велику та успішну компанію без правильно побудованої СУІБ, оскільки безпека даних, а особливо персональних данних користувачів, це найцінніший ресурс яким володіють навіть найменші компанії чи організації, саме вони несуть повну відповідальність в забезпеченні їх бзпеки.

2 СИСТЕМИ УПРАВЛІННЯ/МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ СТАНДАРТУ ISO/IEC 27001

2.1 Сімейство стандарту ISO/IEC 27k. Історичний огляд

Серія стандартів з менеджменту ІБ ISO / IEC 27000 розробляється технічним комітетом ISO / IEC JTC 1 підкомітетом SC 27. СУІБ має в собі вимоги щодо реалізації та вдосконалення систем управління захистом інформації і грунтується на моделі PDCA (Plan-Do-Check-Act):

- створення - ідентифікація активів, управління ризиками;
- впровадження - етапи реалізації відповідних заходів з управління безпекою;
- перевірка - моніторинг та аналіз;
- дію - підтримання в робочому стані та поліпшення.

Не менш важливим елементом системи є забезпечення циклічнос ті усіх процесів з управління безпекою, щоб всі процедури послідовно проходили етапи PDCA. Це свідчить про відповідність системи управління стандарту ISO 27001 і говорить про готовність до сертифікації СУІБ.

Виконання вимог стандарту ISO / IEC 27001 головним чином дає мінімізацію ризиків та втрат активів організації чи підприємства, а отже, на пряму веде до скорочення фінансових втрат.

Стандарт ISO/IEC 27001 призначений для сертифікації систем інформаційної безпеки.

Сертифікація системи управління інформаційною безпекою - це ефективне управління бізнес-процесами підприємства, інформаційними ризиками, а також свідоцтво розвивток та надійність компанії, що в свою чергу дає позитивне ставлення бізнес-партнерів.

СУІБ відповідно до стандарту ISO / IEC 27001 - це частина загальної системи менеджменту компанії. На рисунку 2.3 показано розвиток розвиток створення стандарту ISO/IEC 27001.

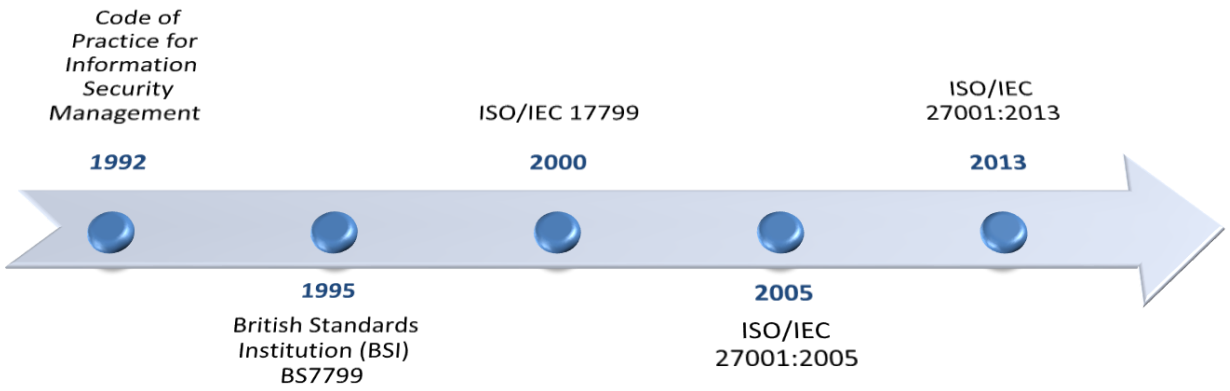

Рисунок 2.2 – Еволюція стандарту ISO/IEC 27001

Тема інформаційної безпеки широко обговорюється і підтверджується в корпоративному середовищі, оскільки інформація вважається одним з найбільш цінних активів для організацій, незалежно від їх сегмента або розміру. Важливість інформації розширила необхідність розробки стандартизованої структури для реалізації і функціонування концепцій інформаційної безпеки. Тому, ISO / IEC ініціювали розробку стандартів, створивши сімейство ICO 27000, яке стандартизує діяльність, пов'язану з впровадженням і експлуатацією систем управління інформаційною безпекою (СУІБ). В таблиц 2.1 описано всі стандарти серії ISO/IEC 27

Таблиця 2.1 – Стандарти сімейства ISO/IEC 27k

Стандарт	Публікація	Назва
ISO/IEC 27000	2018	Системи управління інформаційною безпекою - Огляд та словниковий запас
ISO/IEC 27001	2013*	Системи управління інформаційною безпекою - Вимоги
ISO/IEC 27002	2013*	Кодекс практики контролю захисту інформації
ISO/IEC 27003	2017	Системи управління інформаційною безпекою - Керівництво
ISO/IEC 27004	2016	Управління інформаційною безпекою - моніторинг, вимірювання, аналіз та оцінка
ISO/IEC 27005	2018	Управління ризиками інформаційної безпеки
ISO/IEC 27006	2015	Вимоги до органів, що здійснюють аудит та сертифікацію систем управління інформаційною безпекою
ISO/IEC 27007	2017*	Вказівки щодо аудиту систем управління інформаційною безпекою
ISO/IEC TS 27008	2019	Вказівки щодо оцінки контролю інформаційної безпеки
ISO/IEC 27009	2016*	Застосування ISO / IEC 27001, що стосується сектора - Вимоги
ISO/IEC 27010	2015	Управління інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій

Продовження таблиці 2.1

ISO/IEC 27011	2016	Кодекс практики контролю безпеки інформації, заснований на ISO / IEC 27002 для телекомунікаційних організацій
ISO/IEC 27013	2015*	Керівництво щодо інтегрованого впровадження ISO / IEC 27001 та ISO / IEC 20000-1
ISO/IEC 27014	2013*	Управління інформаційною безпекою
ISO/IEC TR 27016	2014	Управління інформаційною безпекою - Організаційна економіка
ISO/IEC 27017	2015	Кодекс практики контролю захисту інформації, заснований на ISO / IEC 27002 для хмарних сервісів
ISO/IEC 27018	2019	Кодекс практики захисту особистих даних (PII) у публічних хмарах, що виступають як процесори PII
ISO/IEC 27019	2017	Контроль інформаційної безпеки для енергетичної галузі
ISO/IEC 27021	2017	Вимоги до компетенції фахівців із систем управління інформаційною безпекою
ISO/IEC 27022	Розроб.^	Керівництво процесами ISMS
ISO/IEC TR 27023	2015	Картографування оновлених видань ISO / IEC 27001 та ISO / IEC 27002
ISO/IEC 27030	Розроб.^	Керівні принципи безпеки та конфіденційності в Інтернеті речей (IoT)
ISO/IEC 27031	2011*	Керівництво щодо готовності інформаційно-комунікаційних технологій до безперервності бізнесу

Продовження таблиці 2.1

ISO/IEC 27032	2012*	Керівні принципи щодо кібербезпеки
ISO/IEC 27033-1	2015	Безпека мережі - Частина 1: Огляд та концепції
ISO/IEC 27033-2	2012*	Безпека мережі - Частина 2: Вказівки щодо проектування та впровадження мережевої безпеки
ISO/IEC 27033-3	2010*	Безпека мережі - Частина 3: Довідкові сценарії мережевої роботи - Загрози, методи проектування та проблеми управління
ISO/IEC 27033-4	2014*	Безпека мережі - Частина 4: Забезпечення зв'язку між мережами за допомогою шлюзів безпеки
ISO/IEC 27033-5	2013*	Безпека мережі - Частина 5: Захист зв’язку по мережах за допомогою віртуальної приватної мережі (VPN)
ISO/IEC 27033-6	2016	Безпека мережі - Частина 6: Забезпечення доступу до бездротової мережі IP
ISO/IEC 27034-1	2011*	Захист програм - Частина 1: Огляд та концепції
ISO/IEC 27034-2	2015	Захист програм - Частина 2: Нормативна база організації
ISO/IEC 27034-3	2018	Захист програм - Частина 3: Процес управління безпекою додатків
ISO/IEC 27034-4	Розроб.^	Захист програми - Частина 4: Валідація та перевірка

Продовження таблиці 2.1

ISO/IEC 27034-5	2017	Захист програм - Частина 5: Структура даних управління протоколами та безпекою програм
ISO/IECTS 27034-5-1	2018	Захист програм - Частина 5-1: Структура даних управління протоколами та безпекою програм, XML-схеми
ISO/IEC 27034-6	2016	Захист додатків - Частина 6: Приклади
ISO/IEC 27034-7	2018	Захист додатків - Частина 7: Рамка прогнозування достовірності
ISO/IEC 27035-1	2016*	Управління інцидентами інформаційної безпеки - Частина 1: Принципи управління інцидентами
ISO/IEC 27035-2	2016*	Управління інцидентами інформаційної безпеки - Частина 2: Вказівки щодо планування та підготовки до реагування на інцидент
ISO/IEC 27035-3	Розроб.^	Управління інцидентами в галузі інформаційної безпеки - Частина 3: Настанови щодо операцій з реагування на інциденти ІКТ
ISO/IEC 27036-1	2014*	Інформаційна безпека відносин з постачальником - Частина 1: Огляд та поняття
ISO/IEC 27036-2	2014*	Інформаційна безпека відносин з постачальником - Частина 2: Вимоги

Продовження таблиці 2.1

ISO/IEC 27036-3	2013*	Інформаційна безпека відносин з постачальником - Частина 3: Настанови щодо безпеки ланцюга поставок інформаційних та комунікаційних технологій
ISO/IEC 27036-4	2016	Інформаційна безпека відносин з постачальником - Частина 4: Настанови щодо безпеки хмарних послуг
ISO/IEC 27037	2012*	Настанови щодо ідентифікації, збору, придбання та збереження цифрових дока
ISO/IEC 27038	2014*	Специфікація для цифрового редагування
ISO/IEC 27039	2015	Вибір, розгортання та експлуатація систем виявлення та запобігання вторгнень (IDPS)
ISO/IEC 27040	2015	Безпека зберігання
ISO/IEC 27041	2015	Керівництво щодо забезпечення придатності та адекватності методу розслідування інцидентів
ISO/IEC 27042	2015	Вказівки щодо аналізу та інтерпретації цифрових доказів
ISO/IEC 27043	2015	Принципи та процеси розслідування інцидентів
ISO/IEC 27045	Розроб.^	Велика безпека та конфіденційність даних - процеси
ISO/IEC 27050-1	2016*	Електронне відкриття - Частина 1: Огляд та концепції

Продовження таблиці 2.1

ISO/IEC 27050-2	2018	Електронне відкриття - Частина 2: Керівництво для управління та управління електронним виявленням
ISO/IEC 27050-3	2017*	Електронне відкриття - Частина 3: Кодекс практики електронного виявлення
ISO/IEC 27050-4	Розроб.^	Електронне відкриття - Частина 4: Технічна готовність
ISO/IEC 27070	Розроб.^	Вимоги до встановлення віртуалізованих коренів довіри
ISO/IEC 27071	Розроб.^	Рекомендації з безпеки щодо встановлення надійного зв'язку між пристроєм та службою
ISO/IEC 27099	Розроб.^	Інфраструктура публічних ключів - Практика та рамки політики
ISO/IEC TS 27100	Розроб.^	Кібербезпека - огляд та концепції
ISO/IEC TS 27101	Розроб.^	Кібербезпека - керівні принципи розвитку рамок
ISO/IEC 27102	2019	Вказівки щодо кіберстрахування
ISO/IEC TR 27103	2018	Кібербезпека та стандарти ISO та IEC
ISO/IEC TR 27550	2019	Інжиніринг конфіденційності для процесів життєвого циклу системи
ISO/IEC 27551	Розроб.^	Вимоги до автентифікації на основі атрибутів, що не пов'язані між собою

Продовження таблиці 2.1

ISO/IEC 27553	Розроб.^	Вимоги безпеки для аутентифікації з використанням біометричних даних на мобільних пристроях
ISO/IEC 27554	Розроб.^	Застосування ISO 31000 для оцінки ризику, пов'язаного з управлінням особистістю
ISO/IEC 27555	Розроб.^	Встановлення концепції видалення ІПІ в організаціях
ISO/IEC 27556	Розроб.^	Настанова, орієнтована на користувачів, для обробки персонально ідентифікованої інформації (PII) на основі переваг конфіденційності
ISO/IEC 27570	Розроб.^	Правила конфіденційності для смарт-міст
ISO/IEC 27701	2019	Розширення до ISO / IEC 27001 та ISO / IEC 27002 щодо управління інформацією про конфіденційність - Вимоги та рекомендації
ISO 27799 #	2016	Інформатика в галузі охорони здоров'я - Управління інформаційною безпекою в галузі охорони здоров'я з використанням ISO / IEC 27002

^ У стадії розробки; * Переглядається;

Міжнародні стандарти не мають тієї ж загальної назви, але також є частиною сімейства стандартів ISO / IEC 27000

Сімейство стандартів ISO / IEC 27000 складається із взаємопов'язаних стандартів та вказівок, вже опублікованих або в процесі розробки, і містить низку важливих структурних компонентів. Ці компоненти орієнтовані на нормативні стандарти, що описують вимоги до ISMS (ISO / IEC 27001), вимоги органу з сертифікації (ISO / IEC 27006) для тих, хто сертифікує

відповідність ISO / IEC 27001, та додаткові рамки вимог для секторальних впроваджень ISMS (ISO / IEC 27009). Інші стандарти та вказівки містять вказівки щодо різних аспектів впровадження ISMS, що стосуються загального процесу, а також галузевих вказівок.

Міжнародні стандарти, що належать сімейству 27000, служать основою для створення і експлуатації СУІБ.

Мета даного стандарту - зробити загальний огляд системи управління інформаційною безпекою, ознайомивши читачів з технічними термінами, використовуваними в процесі стандартизації.

2.2 Структура та основні засади СУІБ на основі ISO/IEC 27001

Система управління інформаційною безпекою (Information Security Management System, ISMS) – це частка загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов’язки, процедури, процеси і ресурси.

Методи організовані для підтримки процесу визначення, впровадження, експлуатації та обслуговування Системи управління інформаційною безпекою (СУІБ);

– Допомога в управлінні інформаційною безпекою в контексті ризику, управління і управління;
– Приведення у відповідність з концепціями та кращими практиками, прийнятими у всьому світі, без припису, що дозволяє адаптацію відповідно до конкретних потреб кожного бізнесу;
– Довіра до організації з працівниками та ринком;
– Більш ефективне управління інвестиціями в інформаційну безпеку.

Більш значущою метою більшості систем інформаційної безпеки є захист бізнесу та від знищення або витоку інформації. Також однією з основних цілей системи безпеки є гарантія майнових прав та інтересів клієнтів. У той же час способи інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією в компанії, оскільки це може поставити під загрозу розвиток організації.

СУІБ повинна забезпечувати гарантію вирішення таких проблем як забезпечення унеможливості несанкціонованого доступу до критичної інформації, забезпечення конфіденційності критичної інформації, цілісності інформації та пов'язаних з нею процесів (введення, створення, обробки і виведення) і ряду інших цілей.

Досягнення заданих цілей можливо у ході вирішення таких основних завдань, як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки та проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної безпеки, у тому числі методи їх оцінки, контролю інформаційної безпеки на підприємстві. Потрібно зазначити, що тут перераховано не повний список.

Побудова системи управління інформаційною безпекою дозволяє чітко визначити, як взаємопов'язані процеси та підсистеми ІБ, хто за них відповідає, які трудові та фінансові ресурси потрібні для їх ефективного функціонування, і т.д.

Основні функції СУІБ:

- виявлення та аналіз ризиків інформаційної безпеки;
- планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;
- контроль цих процесів;
- внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Якісне управління ІБ базується на наступних принципах:

- комплексний підхід – управління інформаційною системою має бути всеосяжним та охоплювати всі компоненти інформаційнох системи і враховувати всі актуальні ризикоутворюючі фактори, які діють в інформаційній системі підприємства та за її межами;
- узгодженість з бізнес-задачами і стратегією підприємства;
- високий рівень керованості;
- адекватність інформації, яка використовується і генерується;
- ефективність – оптимальний баланс між можливостями, продуктивністю і витратами системи управління інформаційною безпекою;
- безперервність управління;
- процесний підхід – зв'язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, та підтримка нерозривного зв'язку між етапами.

Одним з ключових факторів успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів

ISO/IEC27001.

Стандарт ISO/IEC 27001 дає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої СУІБ в контексті розгляду бізнес ризиків.

СУІБ забезпечує вибір пропорційних та адекватних засобів і методів контролю та захисту інформації, і тим самим, довіру зацікавлених сторін. Але слід брати до уваги й інші стандарти в цій сфері. Зараз у світовій практиці використовують велику кількість стандартів, методик та інших документів, що регламентують процеси управління інформаційною безпекою, наприклад: COBIT, ISM3, ITIL / ITSM, ISO13335-4, BSI-100-2, CRAMM, ISO15408. Просте необхідно зазначити, що всі вони сумісні з ISO 27001 чи подібні до нього. На рисунку 2.4 показано в процентному співвідношенні кількість мір управління по стандарту ISO/IEC 27001

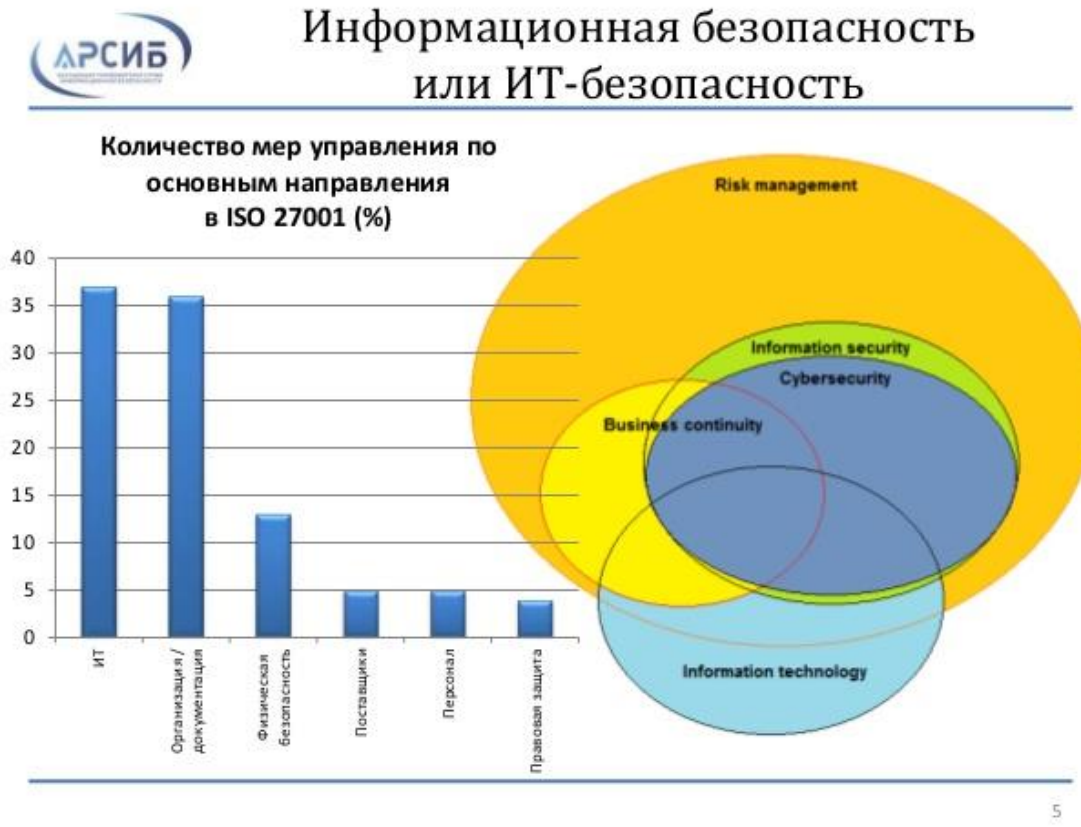

Рисунок 2.4 - Кількість мір управління[19]

Міжнародні організації та інститути, що спеціалізуються у вирішенні комплексних проблем інформаційної безпеки, запропонували концепції проведення аудиту та управління інформаційними ризиками у вигляді міжнародних та національних стандартів: ISO 15408, ISO 27k, COBIT, PCI DSS, SAC, COSO та ін. Зокрема сімейство стандартів ISO 27000 продовжує активно розвиватися та містить стандарти, що визначають вимоги до СУІБ, систему управління ризиками, метрики і вимірювання ефективності механізмів контролю, а також інструкції щодо впровадження. В Україні прийнята серія міжнародних стандартів управління інформаційною безпекою ДСТУ ISO/ IEC 27000:2015. Стандарт визначає інформаційну безпеку як «збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені й інші властивості, такі як автентичність,

неможливість відмови від авторства, достовірність». Конфіденційність — забезпечення доступу до інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі). Цілісність — забезпечення точності і повноти інформації, а також методів її опрацювання. Доступність — забезпечення доступу до інформації авторизованим користувачам, коли це необхідно (на вимогу).

Варто окремо вказати на стратегічні переваги, які може отримати бізнес від сертифікації своєї СУІБ згідно з стандартом ISO 27001:

– побудова надійної структури інформаційної безпеки;

– захист даних та інтелектуальної власності;

– створення нових можливостей (наприклад, співпраця з фінансовими компанія ми);

– підвищення лояльності клієнтів; – уникнення фінансових і репутаційних втрат, пов’язаних з дискредитацією даних;

– зростання довіри інвесторів;

– запобігання кібератакам і витоку даних;

– отримання конкурентної переваги на ринку.

Використовувана в ISO 27001 для опису СУІБ передбачає модель безперервного циклу заходів PDCA (Plan-Do-Check-Act): планування, виконання, перевірка, вплив (управління, коригування), відомий як цикл Шухарта-Демінга дивитись на рис. 2.5 та табл. 2.2.

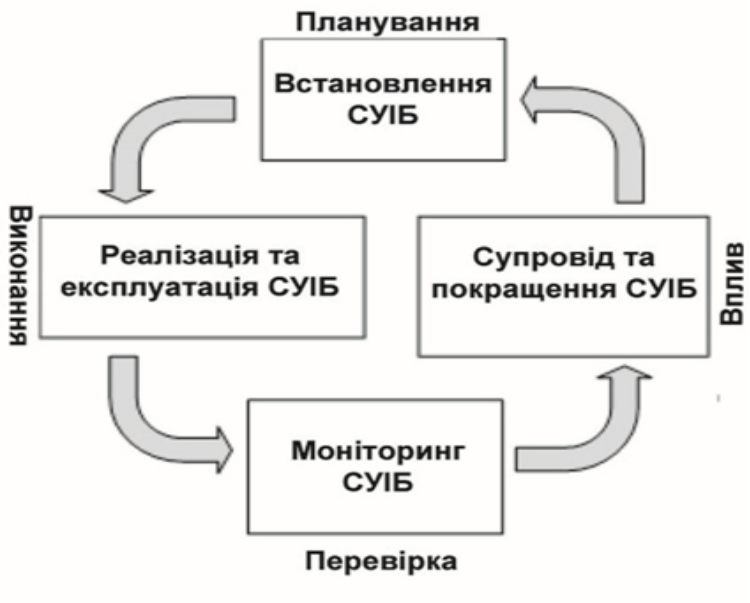

Рисунок 2.5 - Модель PDCA для впровадження СУІБ

Таблиця 2.2 - Опис циклу PDCA для впровадження СУІБ

PDCA	Опис
Планування	Розроблення політики безпеки, визначення мети, процесів та процедур, пов’язаних з управлінням ризиками та підвищенням інформаційної безпеки для досягнення результатів відповідно до загальної політики та цілей організації
Виконання	Впровадження та використання політики безпеки, елементів керування, процесів та процедур, механізмів контролю
Перевірка	Оцінювання та вимірювання ефективності роботи відповідно до політики безпеки, цілей та практичного досвіду, а також підготовка звіту про результати для керівництва з метою подальшого аналізу й аудиту
Вплив (управління, коригування)	Застосування коригувальних та профілактичних заходів з метою досягнення постійного вдосконалення СУІБ на основі результатів аналізу; перегляд політики безпеки; підвищення поінформованості персоналу

Побудова системи управління інформаційною безпекою — це комплексний процес, направлений на мінімізацію зовнішніх і внутрішніх загроз із врахуванням обмежень на ресурси і час. Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності, потім визначити поріг ризику, тобто рівень загрози, при якому вона потрапляє в процес управління ризиками. Отже, потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику.

Зважаючи на сукупність бізнес-процесів, специфіку інформаційного продукту, переважно мультимедійного видання, з методологічного погляду, створення СУІБ може бути реалізовано в такі шість ета пів (рис. 2.6), а з позиції процесного підходу систему інформаційної безпеки можна представити як процес управління ризиками (рис. 2.7), як ключового етапу управління ІБ.

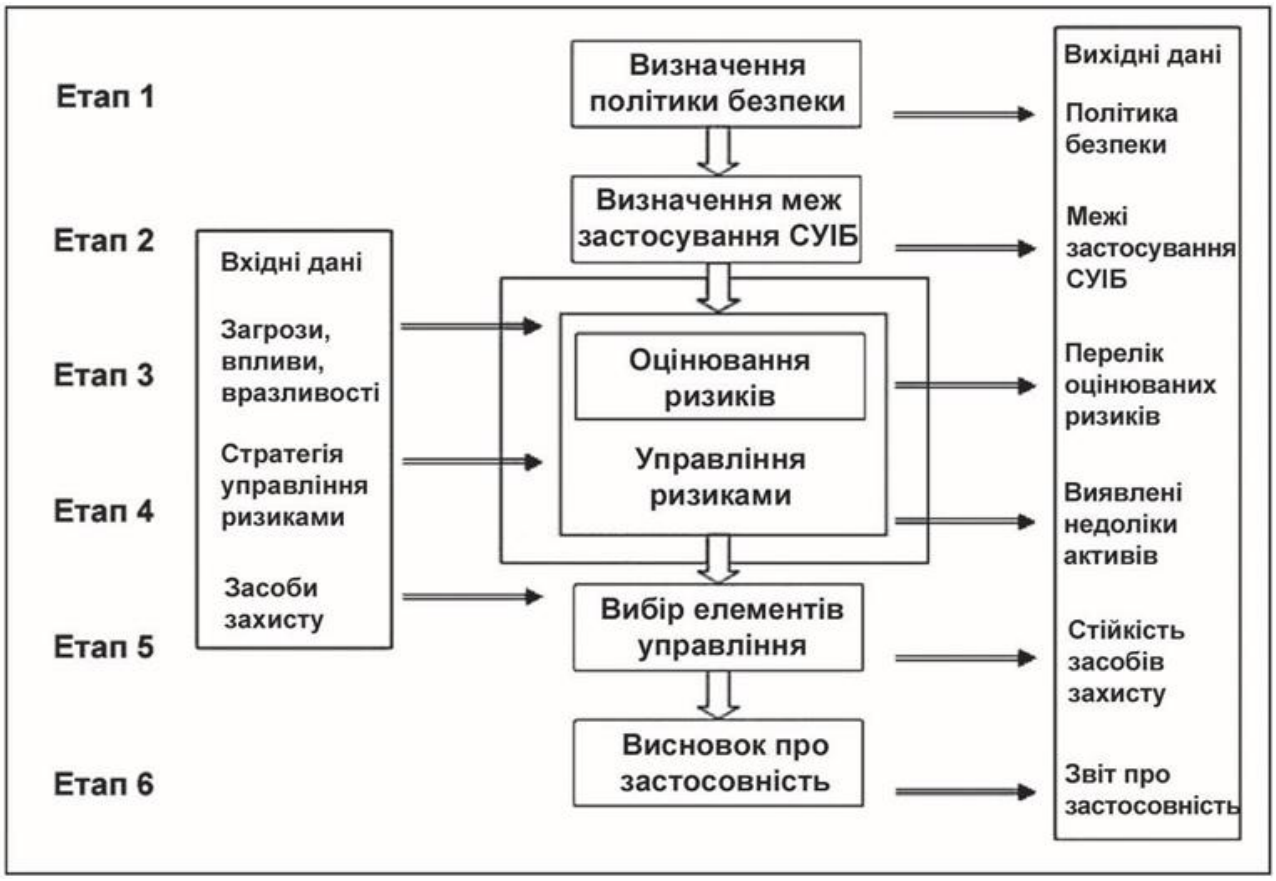

Рисунок 2.6 - Етапи процесу створення СУІБ

Етапи 3 і 4 утворюють основу СУІБ і є процесами, які трансформують принципи політики безпеки організації, а також перетворюють цілі СУІБ в конкретні плани щодо впровадження механізмів керування і захисту, спрямованих на мінімізацію загроз і вразливостей. Процедури та дії на етапах 5 та 6 не стосуються інформаційних ризиків. Вони радше пов'язані з оперативними діями, необхідними для технічної реалізації, обслуговування і управління, оцінюванням рівня безпеки. Відповідні засоби контролю можна отримати з існуючих наборів засобів чи механізмів, які зазвичай містяться в стандартах та керівних положеннях інформаційної безпеки, або як результат поєднання чи адаптації пропонованих засобів до конкретних вимог організації та експлуатаційних характеристик. В обох випадках етап 6 є задокументованим відображенням виявлених ризиків в умовах конкретного редакційно-видавничого процесу, що містить технічну реалізацію механізмів безпеки, які планують застосувати. Незважаючи на те, що СУІБ є циклічним процесом, у більшості компаніях етапи 1 та 2 повторюватимуться рідше, ніж етапи 3, 4, 5 та 6. Це пов'язано з тим, що створення політики безпеки та визначення меж СУІБ є управлінськими та стратегічними питаннями, тоді як процес управління ризиками - це щоденна операційна проблема.

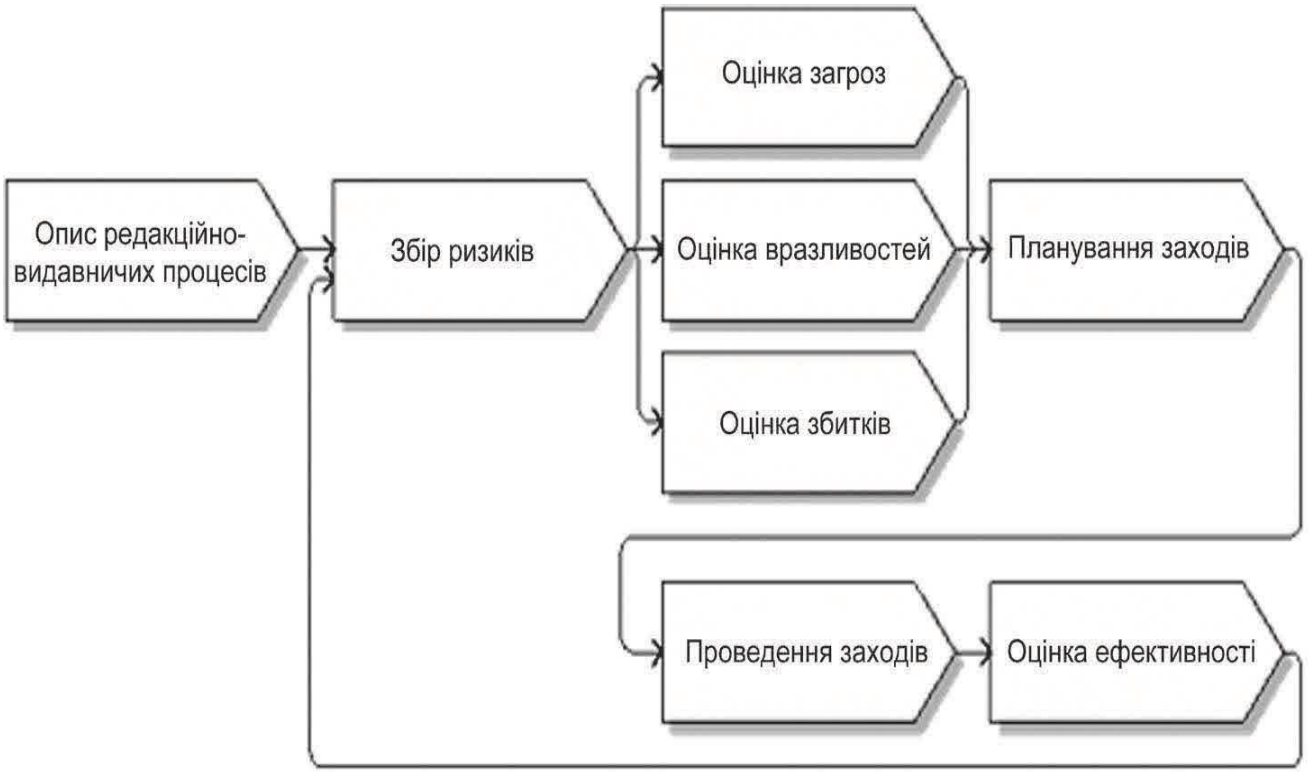

Рисунок 2.7 - Модель системи управління ризиками для СУІБ

Аналіз моделі управління ризиками потребує розгляду в рамках узагальненої моделі системи інформаційної безпеки, із розкриттям таких понять як об’єкт захисту, види і модель загроз, модель порушника і т.д.

2.3 Висновки до розділу 2

В цьому розділі описана структура сімейства стандарту ISO/IEC 27k. Описано те, як створювався стандарт, передумови його виникненню. Були розглянуті основні етапи його розвитку та становлення на міжнародній арені стандартів з інформаційної безпеки. Також було розглянуто основну структуру та засади системи управління інформаційної безпеки. Описано, які компоненту безпеки входять в структури, організація та впровадження СУІБ.

3 ДОСЛІДЖЕННЯ ПРОБЛЕМ ВПРОВАДЖЕННЯ ТА СЕРТИФІКАЦІЇ СУІБ НА ОСНОВІ ISO/IEC 27001

3.1 Органи оцінки відповідності („ООВ”) на основі ISO/IEC 27001 та їх місце в глобальній інфраструктурі якості

Органи з оцінки відповідності

Існують різні типи органів з оцінки відповідності (ООВ), які можуть здійснювати методи та заходи щодо оцінки відповідності. Вони можуть мати будь-яку організаційну форму та форми власності, і можуть бути комерційними чи неприбутковою організацією. Вони можуть бути державними установами, національними органами з питань стандартизації, торговими асоціаціями, споживчими організаціями або приватними або державними компаніями.

Органи з оцінки відповідності варіюються від багатомільярдних багатонаціональних компаній, які здійснюють всі види діяльності з оцінки відповідності (наприклад, тестування, інспектування та сертифікація), до ООВ, що пропонують національні послуги в одній конкретній країні, або невеликих локалізованих організацій, які працюють у певному секторі та регіоні. У більшості випадків ООВ можуть виступати першою, другою чи третьою стороною, яка організовує оцінку відповідність певної організації, компанії то щ . Якщо органи діють у якості сторонніх осіб, важливою особливістю є те, що вони повинні діяти неупереджено, щоб результати їх роботи могли бути об'єктивними та підтримувати найвищу ступінь відповідності.

Забезпечення діяльності з оцінки відповідності ООВ, як правило, базується на платі за послугу, яка може або не може відображати рентабельність інвестицій або прибуток. У багатьох країнах є конкурентоспроможний ринок серед ООВ для проведення заходів з оцінки відповідності. Однак у деяких країнах монополія належить одній або декільком визнаним урядом органам з оцінки відповідності, положеннями чи

методами закупівель. В таблиці 3.1 показано яким ООВ які стандарти відповідають.

Таблиця 3.1 – Перелік органів оцінки відповідності

Органи оцінки відповідності	Міжнародний стандарт
Випробувальні лабораторії	ISO / IEC 17025
Інспекційні органи	ISO / IEC 17020
Органи сертифікації осіб	ISO / IEC 17024
Органи сертифікації продуктів процесів та послуг	ISO / IEC 17065
Органи сертифікації систем управління	ISO / IEC 17021

Структура вищезазначених Міжнародних стандартів схожа тим, що вони містять як технічні, так і організаційні вимоги:

- загальні вимоги - наприклад юридичні та договірні питання;
- структурні вимоги - наприклад конкретні організаційні структури, які повинні існувати;
- вимоги до ресурсів - вимоги до компетенції, обладнання та робочого середовища, а також вимоги субпідрядів / аутсорсингу;
- записи та вимоги до інформації - наприклад збереження документів і записів, конфіденційність та доступність;
- вимоги до процесу - вимоги до конкретної діяльності з оцінки відповідності;
- Вимоги до системи управління - вимоги до внутрішнього управління ООВ для забезпечення його загального виконання відповідного Міжнародного стандарту.

Вищенаведені Міжнародні стандарти містять вимоги, пов’язані з темами, які є більшою чи меншою мірою загальними для всіх органів з оцінки відповідності, таких як:

- неупередженість
- конфіденційність
- скарги та звернення
- публічне оприлюднення;
- використання систем управління ООВ.

При використанні стандартів ISO27x, організації можуть реалізовувати і поліпшувати СУІБ та підготуватися до незалежної оцінки їх СУІБ в органах оцінки відповідності, які є акредитованими та визнаними в міжнародній системі акредитації International Accreditation Forum (IAF), наприклад, Європейською асоціацією з акредитації (ЄА). Далі під СУІБ будемо розуміти саме таку систему, що створена у відповідності до вимог стандартів серії ISO27x.

Сімейство міжнародних стандартів СУІБ ISO27k розробляє Об'єднаний технічний комітет ISO/IEC JTC 1, підкомітет SC 27 «Методи захисту ІТ» (ISO/IEC JTC 1/SC 27 «Методи і засоби забезпечення безпеки інформаційних технологій» (англ.: – IT Security techniques). Загальна кількість опублікованих стандартів ISO під прямою відповідальністю ISO/IEC JTC 1/SC 27 – 137 стандартів, в тому числі стандартів ISO27x – 28. Стандарти ISO27x можуть бути класифіковані за рівнями ієрархії, як відображено на Рис. 1. При цьому перші три рівні ієрархії можна об’єднати поняттям системостворюючих стандартів або стандартів вищих рівнів. Всі інші стандарти ISO27x, які знаходяться на четвертому і, можливо, нижчих рівнях, об’єднаємо поняттям стандартів прикладних рівнів. На рисунку 3.1 схематично зображено ієрархую стандатів серії ISO/IEC 27k

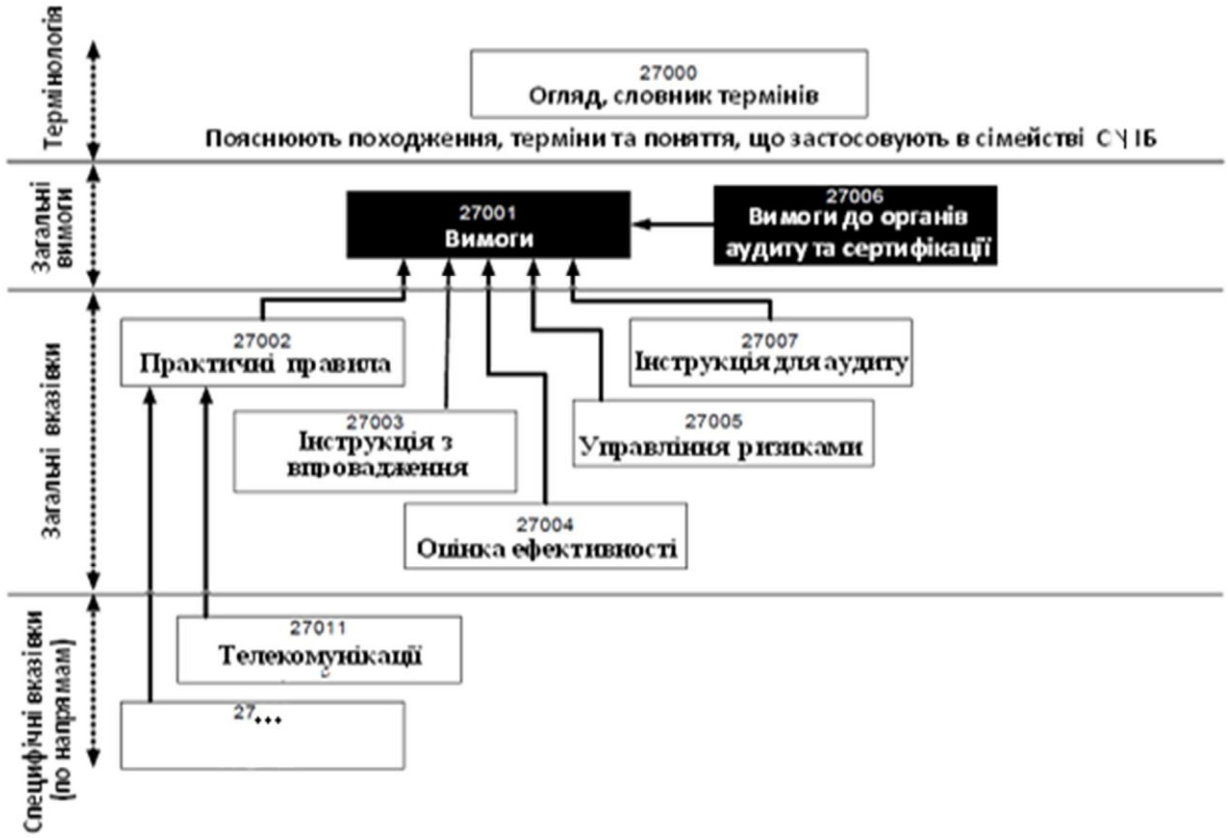

Рисунок 3.1 - Ієрархія стандартів СУІБ (ISMS – Information Security management systems)

ISO/IEC 27001:2015 «Інформаційні технології. Стандарт вищого рівня. Методи та засоби досягнення інформаційної безпеки. Системи управління інформаційною безпекою. Вимоги» (англ.: Information technology – Security techniques. Information security management systems – Requirements). Цей стандарт є базовим стандартом ISO27k. ISO/IEC 27001 визначає вимоги для створення, впровадження, експлуатації, моніторингу, аналізу, підтримки і поліпшення документованої СУІБ в контексті загальних ризиків організації бізнесу. Цей стандарт призначений для забезпечення вибору адекватного і пропорційного контролю систем інформаційної безпеки. Стандарт ISO/IEC 27001 призначений для сертифікації СУІБ в ООВ. В Україні ООВ, який здійснює сертифікацію СУІБ, з можливістю визнання сертифікату за межами країни повинен бути акредитованим національним органом з акредитації, яким з 2002 року є Національне агентство з акредитації України (НААУ) і

якому надані державні ексклюзивні повноваження на акредитацію ООВ та проведення моніторингу за відповідністю акредитованих ним ООВ вимогам акредитації. На сьогодні в реєстрі НААУ вже є ООВ, акредитовані згідно стандарту ISO/IEC 17021:2011 «Оцінка відповідності. Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту (англ.: Conformity assessment – Requirements for bodies providing audit and certification of management systems) щодо компетентності здійснювати сертифікацію СУІБ відповідно до стандарту ISO/IEC 27001. Сертифікована СУІБ – гарантія того, що СУІБ правильно і ефективно впроваджена в область діяльності організації. А ефективна СУІБ, у свою чергу, забезпечує необхідний рівень захисту активів організації, тобто істотно знижує ризик нанесення організації збитку внаслідок порушення інформаційної безпеки і гарантує, що міри і кошти захисту інформації є адекватному і пропорційними можливому збитку організації. Сертифікація на відповідність цього стандарту дозволяє наочно показати діловим партнерам, інвесторам і клієнтам, що у організації налагоджене ефективне управління інформаційною безпекою.

3.2 Акредитація ООВ СУІБ на основі ISO/IEC 27001

Акредитація - це процедура, підчас якої нац. орган з акредитації засвідчує компетентність юридичної особи чи відповідного органу з оцінки відповідності виконувати певні види робіт (калібрування, випробування, контроль, сертифікацію,).

Акредитація надає:

- забезпечення однієї технічної політики у сфері оцінки відповідності в країні;
- забезпечення довіри споживачів до результатів діяльності ООВ;
- забезпечення умов для взаємного визнання результатів діяльності акредитованих органів на міжнародному рівні;
- усунення технічних бар’єрів для бізнесу.

В Україні орган який займається акредитацією органів оцінкою відповідності є національна агенція з акредитації України (НААУ). Під час акредитації НААУ керується рекомендаціями міжнародних організацій ILAC та IAF та регіональної ЕА організацій з акредитації. Структура НААУ з її підрозділами зображена на рис.3.1.

,,Закон України “Про акредитацію органів з оцінки відповідності” був ратифікований в 2001р., тим самим були визначені законодавчі, організаційні та економічні заходи для акредитації органів з оцінки відповідності в Україні. Відповідно до нього, у січні 2002р. Міністерство економіки України створило Національне агентство з акредитації України (НААУ). Окрім цього, були створені Рада з акредитації, Технічний комітет з акредитації та Комісія з апеляцій. Закон 2001р. передбачає та дозволяє створити більшу кількість Технічних комітетів з акредитації.

Головними функціями Національного агентства з акредитації України є акредитація органів з оцінки відповідності та подальший контроль над відповідністю акредитованих органів вимогам акредитації. Агентство працює, посилаючись на стандарт ISO / IEC 17011 та процедури міжнародних професійних організацій. Воно підписало угоди з співробітництва з: Європейською кооперацією з акредитації, міжнародним форумом з акредитації та міжнародною кооперацією з акредитації лабораторій, Однак головним завданням НААУ як частини національної Інфраструктури якості та системи технічних регламентів є приєднання до ЕА у таких секторах: органи сертифікації продукції, органи сертифікації систем менеджменту, калібрувальні та випробувальні лабораторії. У листопаді 2009р. під час засідання Комітету багатосторонньої угоди ЕА було вирішено надати НААУ визнання в області "сертифікації персоналу”, що дозволяє вирішити питання визнання в інших областях акредитації у доступному для огляду майбутньому“ [19]. В таблиці 3.2 зображено реєстр усіх акредитованих ООВ

Таблиця 3.2 - Реєстр акредитованих ООВ в Україні

Назва	Кількість діючих атестатів про акредитацію	Кількість не діючих атестатів про акредитацію	Загальна кількість
Випробувальнілабораторії (ДСТУ ISO/IEC 17025)	777	357	1134
Калібрувальні лабораторії (ДСТУ ISO/IEC 17025)	31	6	37
Медичні лабораторії (ДСТУ EN ISO 15189)	13	0	13
Провайдери програм перевірки кваліфікації (ДСТУENISO/IEC 17043:2017)	4	0	4
Органи з сертифікації продукції, процесів та послуг(ДСТУ EN ISO/IEC 17065)	120	48	168
Органи з сертифікації персоналу (ДСТУ EN ISO/IEC 17024)	14	0	14
Органи з інспектування (ДСТУ EN ISO/IEC 17020)	94	73	167
Органи з сертифікації систем менеджменту (ДСТУ EN ISO/IEC 17021-1)	60	22	82
В цілому	1113	506	1619

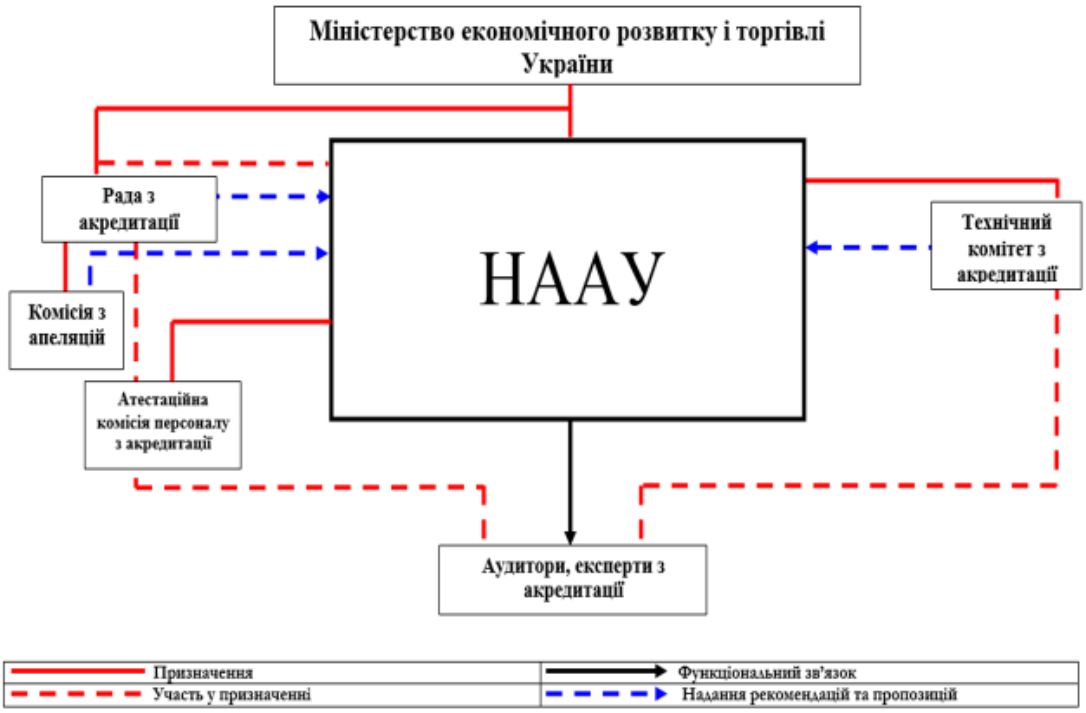

Рисунок 3.2 – Структура організації управління НААУ

Оцінка відповідності – це процес, який здійснюється виробником для демонстрації того, що встановлені вимоги стосовно продукції були виконані.”

Виробник завжди є відповідальним за оцінку відповідності що до якості свого продукту. Продукція підлягає оцінці відповідності на кожному етапі виробництка.

Існує 3 варіанти проведення ООВ:

1. Без залучення третьої сторони.

Це може стосуватись випадку, коли декларації виробника (що супроводжується відповідними технічними експертизами та документацією) достатньо, щоб забезпечити відповідність конкретної продукції відповідним законодавчим вимогам. У цьому випадку виробник сам здійснює всі

необхідні контрольні заходи та перевірки і складає технічну документацію, а також забезпечує відповідність процеса виробництва.

2. З залученням акредитованого органу оцінки відповідності, що підпорядковується компанії та є частиною організації виробника.

Такий внутрішньофірмовий орган не повинен здійснювати жодної іншої діяльності, ніж оцінка відповідності, та повинен бути незалежним від будь-яких комерційних, проектувальних чи виробничих підрозділів. Він повинен продемонструвати той же рівень технічної компетентності та неупередженості, що й зовнішні органи з оцінки відповідності, шляхом акредитації.Там, де це необхідно для конкретного сектора, законодавець може взяти до уваги той факт, що виробники використовують добре обладнані випробувальні лабораторії чи приміщення, а їхня компетентність може бути вищою, ніж можливості деяких зовнішніх органів. Це може стосуватись нової інноваційної складної продукції, для якої найсучасніші науково-технічні знання щодо випробувань залишаються у виробників.

3. З залученням третьої сторони. Зовнішнього органу з ООВ.

У деяких інших випадках законодавець може вважати за необхідність залучення третьої сторони, тобто зовнішнього органу з оцінки відповідності. Такий орган повинен бути неупередженим і повністю незалежним від організації або продукції, яку він, він не може займатись будь-якою діяльністю, яка може вплинути на його незалежність, таким чином, він не може мати інтересів користувача або інших інтересів стосовно продукції, яка має бути ним оцінена.

Нотифіковані органи **є** органами з оцінки відповідності, які були офіційно призначені своїм національним органом влади для здійснення процедур оцінки відповідності і виконують завдання щодо процедур оцінки відповідності, які встановлені в застосовному технічному гармонізованому законодавстві, коли вимагається залучення третьої сторони.

3.3 Стан впровадження та сертифікації СУІБ ISO\IEC 27001 в Україні

У 2005 році Міжнародною організацією зі стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC) був розроблений і прийнятий стандарт ISO 27001-2005. Стандарт ISO 27001 містить вимоги в області інформаційної безпеки для створення, впровадження і розвитку СМІБ підприємства. У стандарті ISO 27001 зібрані кращі світові практики в галузі ІБ. Система інформаційної безпеки підприємства має демонструвати здатність організації до захисту своїх інформаційних ресурсів. Стандарт ISO 27001 визначає впровадження, моніторинг, аналіз, функціонування, підтримку і СМІБ. Стандарт ISO 27001 по багатьох моментах гармонізований і містить схожі вимоги з стандартом ISO 9001. Тому підприємства, які розробляють СУІБ можуть впровадити інтегровану систему, яка відповідає вимогам стандартів ISO 27001 і ISO 9001.

В 2014 році стандарт ДСТУ ISO 27001-2014 «Інформаційні технології, Методи безпеки був прийнятий Україною. Системи менеджменту інформаційної безпеки. Вимоги. », Який по суті є перекладеної копією стандарту ISO 27001-2013. Стандарт був прийнятий, оскільки, цього вимагали домовленості взяті Україні перед Європейським союзом, коли була підписана угода про асоціацію.

До ратифікації угоди, стандарт ISO/IEC 27001 використовувався лише галузевими органіціями, компаніями. Не путати з ДСТУ ISO 27001-2014.

Організації, які були сертифікованими стандартом ISO/IEC 27001, були наприклад Національний Банк України, який ще у 1998 році почав використовувати вимоги цього стандарту і випустив так звану постанову №95. На сьогоднішній день остання редакція постанови здійснена за 28.09.2017 та звучить як „ Постанова про затвердження положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України “. Крім банківської сфери, сертифікація за ISO/IEC 27001

здійснювалась ще в декількох сферах державного регулювання держави, а саме в енергетичному, промисловому та секторі будівництва.

В ході історичного розвитку, Україна, за для більш прозорої співпраці з іншими країнами у різних сферах, почала запроваджувати світові стандарти ДСТУ ISO/IEC 27000:2019, ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2015 і так далі. Всі ці стандарти є повністю перекладеними варіантами з міжнародних стандартів ISO/IEC 27k, які є показником якості, довіри та безпеки співпраці у сьому світі.

3.4 Шляхи вдосконалення національної системи інформаційної безпеки за стандартом ISO/IEC 27001

Головною метою нашої держави на сьогоднішній день є подальше впровадження міжнародного стандарту інформаційної безпеки ISO/IEC 27001 в різні сфери діяльності держави, як в приватному так і державному секторі. Дуже важливим є те, щоб Україна як в найкоротші строки прийняла як найбільшу кількість галузевих стандартів ISO/IEC 27k на основі ДСТУ. Крім цього, важливим етапом вдосконалення національної системи ІБ буде контроль за виконанням усіх вимог стандартів та своєчасне впровадження оновлених версій стандартів.

Вдосконалення системи інформаційної безпеки, дасть змогу не тільки державі отримувати преференції в різних сферах діяльності, а в першу чергу для пересічних Українців. Для прикладу візьмемо інцидент який нещодавно сколихнув не тільки всіх українців, але й увесь світ. Тією чи іншою мірою всі ми, не залежно від соціального статусу та місця в суспільстві, відчули його наслідки. 27 червня 2017 року була здійснена масштабна атака з боку Росії проти України. Вірус під назвою „Петя“ вивів з ладу або спричинив порушення роботи українських державних та приватних установ, підприємств, медіа, баків та завдав великої шкоди для малого та середнього бізнесу. В ході атаки була заблокована діяльність великої кількості компаній

та підприємств: Укртелеком Укрпошта, ворота нашої держави аеропорт ,,Бориспіль” , Укрзалізниця, атомні станції, урядові установи та багато інших. Відповідальність за атаку повною мірою поклали Росію всі п'ять країн-членів союзу FVEY.

Саме не бачення проблем до ситуації 22 червня 2017 року, через застарілість національної системи інформаційної безпеки, не бажання вищих чинів влади в модернізації систему, а в деяких випадках просто не компетенція відповідних органів призвела до цієї трагедії.

Якщо подивитись на хронологію подій, саме після цього, і телевізійному та радіо просторі почали говорити за якнайшвидше впровадження міжнародного досвіду, перекваліфікацію спеціалістів та запровадження нових систем управління національної СУІБ.

До проблеми потрібно підійти кардинально. Запровадження новітніх стандартів у сфері інформаційної безпеки – це запорука безпеки кожного громадянина та держави в цілому. Без сучасних засобів безпеки інформації, країна може нести багато мільярдні збитки, що несе за собою економічний крах, а в деяких випадках навіть і суверенітету.

3.5 Висновки до розділу 3

У розділі 3 досліджувались проблеми впровадження та сертифікації СУІБ на основі стандарту ISO/IEC 27001.

Узагальнюючи все вище сказане, Україна іде на правильному шляху розвитку інформаційної безпеки. Органи оцінки відповідності розташовані по всій території нашої країни і будь-хто може без перешкод скористатись їх послугами в будь-який момент в тій галузі, яка потрібна особисто для нього. Акредитацію органів в Україні здійснює НААУ, яке є повністю компетентне в цих питаннях, оскільки перевіряється всесвітньо визнаною ЕА.

Що до вдосконалення СУІБ, через співпрацю країни з західними партнерами, від нас вимагають запровадження сучасних стандартів у всіх

сферах державного регулювання та управління, ні в якому разі не може погано вплинути на життєдіяльність держави, у більшості випадках, це є великим кроком вперед у деяких сферах.

ВИСНОВКИ

Сьогодні, ми живемо в глобалізованому світі, де кордони між державами, можна вважати лише умовною лінією розподілу, а відстань між Києвом та Лондоном за останні 300 років фактично скоротилась до трьох з половиною годин. Це не може нас не тішити. Але, разом з сучасними досягненнями людства, приходять нові загрози.

Проблеми в інформаційній безпеці спіткають кожного з нас, тією чи інщою мірою, кожного дня. Більшість людей навіть не задумуються над всією повнотою проблеми. Інформаційна безпека, отримала друге дихання після розповсюдження Інтернету по всьому світу. Станом на 2018 рік, кількість активних користувачів Інтернет сягнула позначки 4 мільярди чоловік, а станом на лютий місяць 2020 року їх кількість перевищила 4,5 мільярда, тобто кількість користувачів зросла на 7% (298 мільйонів нових користувачів) більше порівняно з січнем 2019 року. А отже, проблема як ніколи серйозна.

Міжнародні стандарти безпеки, такі як ISO/IEC 27k, покликані забезпечити нас від загроз, які виникають в сучасних реаліях. Ці стандарти, були створені та впроваджені в СУІБ різних країн, організацій, компаній, багато років назад, та весь час оновлюються. В них зібрані найкращі практики для забезпечення безпеки, які пройшли випробування часом. Їх запровадження, дозволяє забезпечити найкращу недоторканність конфіденційних, особистих даних від зловмисників, їх дотримання допоможе мінімізувати втрати, які будуть нанесені при вдалій атаці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ИНФРАСТРУКТУРА КАЧЕСТВА ТОРГОВЛЯ, ОСНОВАННАЯ НА ДОВЕРИИ. ООН по промышленному развитию
file:///C:/Users/Just%20Joy/Downloads/QI_Russian_online_final_0.pdf
2. Вадим Гребеніков «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ. СТАНДАРТЫ СУИБ»
https://mybook.ru/author/vadim-grebennikov-2/upravlenie-informacionnoj-bezopasnostyu-standarty/read/
3. https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/
4. International Journal of Recent Contributions from Engineering, Science & IT (iJES) – eISSN: 2197-8581 https://online-journals.org/index.php/i-jes/article/view/2937/2874
5. https://intercert.com.ua/articles/regulatory-documents/210-iso-27000
6. https://ostec.blog/en/general/first-steps-iso-27000
7. https://www.ogcio.gov.hk/en/our_work/information_cyber_security/collaboration/doc/overview_of_iso_27000_family.pdf
8. https://www.slideshare.net/CHS2410/iso27k
9. https://www.slideshare.net/CHS2410/iso27k
10. file:///C:/Users/Just%20Joy/Downloads/11.pdf
11. https://www.iso.org/sites/cascoregulators/01_3_conformity-assessment-bodies.html#laboratories
12. з книги О.О. Цвілій. Телекомунікаційні та інформаційні технології
file:///C:/Users/Just%20Joy/Downloads/249-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-961-1-10-20141130.pdf
13. https://naau.org.ua/nacionalne-agentstvo-z-akreditaciyi-ukrayini/struktura-nacionalnoyi-sistemi-akreditaciyi/
14. https://naau.org.ua/reyestr-akreditovanix-oov/

15. https://helpdesk.epo.org.ua/article/ocinky-vidpovidnosti
16. http://www.standardacademy.org/wp-content/uploads/2017/04/ASSESMENT-AND-ACCREDITATION_ukr.pdf
17. https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/]
18. https://www.slideshare.net/CHS2410/iso27k
19. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjVnPOUwPLpAhXqkIsKHUqIAL0QFjAAegQIBBAB&url=http%3A%2F%2Fwww.standardacademy.org%2Fwp-content%2Fuploads%2F2017%2F04%2FASSESMENT-AND-ACCREDITATION_ukr.pdf&usg=AOvVaw1iRi8tIuGgbNnwxdBr8C9Q